世界数学名题欣赏丛书

置换多项式及其应用

孙 琦 万大庆 著

辽宁教育出版社

1987年·沈阳

置换多项式及其应用

孙　琦　万大庆 著

辽宁教育出版社出版　辽宁省新华书店发行
（沈阳市南京街6段1里2号）朝阳新华印刷厂印刷

字数：57,000　开本：787×1092 1/32　印张：4 1/2　插页：4
印数：1—4,500
1987年10月第1版　　1987年10月第1次印刷

责任编辑：俞晓群　谭　坚　　责任校对：王淑芬
封面设计：安今生　　　　　　插　　图：安　迪

统一书号：7371·499　　定价：1.20 元
ISBN 7-5382-0171-X

内 容 简 介

本书是“世界数学名题欣赏丛书”之一。置换多项式就是可表达完全剩余系的多项式。完全剩余系问题是1801年由数学家高斯在他的著作《算术探讨》中首先提出的，这一问题在数论研究中占有非常重要的地位。而置换多项式问题又在完全剩余系研究中占有重要地位。本书系统地介绍了置换多项式的产生、发展和理论，并且着重介绍了它在现代科学中的广泛应用。论述深入浅出，简明生动，读后有益于提高数学修养，开阔知识视野。

Summary

This book is one of A Series of World Famous Mathematics-Appreciation. Permutation polynomial is the polynomial that can express complete residue classes. The problem of complete residue classes was first put forward by mathematician Gauss in his work «Disguisition Arithematicae» in 1801. This problem occupies an important place in the mathematic research. However, the problem of permutation holds an important place in the research of complete residue classes. The book systematically introduces the birth, development and theory of permutation polynomials, and mainly introduces its wide application in modern science. Its exposition explains the profound in simple terms with concise and vivid language. After reading it, we can raise our understanding of mathematics, and widen our knowledge field of vision.

前　言

什么是置换多项式？简单地讲，置换多项式就是表完全剩余系的多项式。历史上，完全剩余系起源于数学王子高斯的工作，早在1801年，在他的名著《算术探讨》中就有对完全剩余系的系统研究。

什么又是完全剩余系呢？设m是一个正整数，我们知道任何一个整数用m去除后其余数均在$\{0,1,\cdots,m-1\}$中。若有m个整数，其余数正好互不相同（因此取$\{0,1,\cdots,m-1\}$中的每个数正好一次），则称这m个数组成的集合为模m的一个完全剩余系。又设a，b是任意整数，$(a,m)=1$，如果x通过模m的一个完全剩余系，则$ax+b$也通过模m的一个完全剩余系，这是数论中一个熟知的性质。注意，$ax+b$是一次整系数多项式。于是自然要问：若$f(x)$是一个n次整系数多项式，那么当x通过模m的一个完全剩余系时，

$f(x)$是否也通过模m的一个完全剩余系？若结论是肯定的，则称$f(x)$是模m的一个置换多项式。

1863年，厄米特首先开创了对模p（p是素数）的置换多项式的研究，得出了判别置换多项式的准则。1866年和1870年，塞利特和约当分别作了进一步的工作.之后，迪克逊于1896年—1897年将置换多项式的概念推广到任意有限域上，对置换多项式作了深入和系统的探讨，这些工作的一个概述可以在他1901年的著作《线性群》中找到。1923年，迪克逊在他的名著《数论史》第三卷中总结了1922年以前有关置换多项式的结果。这一时期的基本工作均是由迪克逊本人完成的。

本世纪五十年代以来，卡里兹及其学生，还有其他一些数学家对置换多项式又开始了新的研究。一些深入的工具，如黎曼曲面的理论，代数数论,算术代数几何等相继用到置换多项式上,得出了许多深刻的结果。模p的单变元置换多项式也开始被推广到剩余类环以至一般环的多变元置换多项式上，这些工作大大丰富了置换多项式的内容，给该领域以极大的推动和发展。1973年，劳斯基和诺鲍尔在其专著《多项式代数》中收入了一百余篇关于置换多项式的论文。到1983年，从利德尔和利德奈特的百科全书式的著作《有限

域》一书中可以看出，研究置换多项式的论文已多达四百余篇！可见，近年来，置换多项式发展相当迅速。

引起置换多项式迅速发展的一个原因是置换多项式已逐渐在数论，组合论，群论，非结合代数，密码系统等领域中得到应用。作为一个有趣的例子，我们在第二章中将给出置换多项式对公开密钥码的一个应用。

应当指出，对置换多项式的研究虽有一百余年的历史，该领域内仍有大量的工作可做，还有许多问题没有得到解决，对于一般环上的置换多项式更是如此。

鉴于上述情况及国内目前尚无介绍这方面工作的读物，我们特将有关置换多项式的基本内容及进展情况整理成册，用尽量简单的形式介绍给我国读者，以促进国内在这方面的研究。在材料的选取上，我们仅限于模m的置换多项式和有限域F_q上的置换多项式，因为这两种情形都是最简单和基本的，都有比较丰富和完善的结果，而且得到了较广泛的应用。所以这种选取并不影响对置换多项式这个课题的了解。对于一般的抽象环上的置换多项式及多变元置换多项式，读者可参考文献〔24〕和〔27〕，后者附有非常完备的参考文献。

另外，对不太复杂的定理，我们都尽量给出其证明，这样，通过本书读者不仅能够了解到置换多项式的一个概貌，而且能学到一些基本的解决问题的方法。我们在书中还提出了一些有待解决的问题，以供有志于在这方面进行研究的读者参考。在附录中，我们还不加证明地介绍了用到的一些预备知识，因此，读者只要具备代数的基础知识，就能读懂本书的绝大部分内容。

最后，由于这本小册子首次将有关置换多项式的基本内容整理成册，限于作者的水平，错误和不妥之处在所难免，敬请读者批评指正。

作　者

1986年9月于成都

世界数学名题欣赏丛书

费马猜想

黎曼猜想

连续统假设

希尔伯特第十问题

欧几里得第五公设

哥德尔不完全性定理

不动点定理

无处可微的连续函数

科克曼女生问题

斐波那契数列

哥德巴赫猜想

置换多项式及其应用

素数判定与大数分解

货郎担问题



作 者 简 介

孙琦（左），1937年生于浙江省吴兴县，1961年毕业于四川大学数学系，现为四川大学数学系教授、数学研究所数论研究室主任、《数学学报》编委、四川省数学会副秘书长。已发表学术论文50余篇，出版著作五种，有：《单位分数》，《谈谈不定方程》，《初等数论100例》，《数论讲义》（上），《快速数论变换》，总共约七十余万字（包括合作）。主要研究方向为数论中的不定方程和应用数论。

万大庆，1964年生于四川重庆，1982年毕业于成都地质学院基础部，1982——1986年在四川大学数学系攻读博士学位，现在美国华盛顿大学数学系学习。已发表论文15篇，主要研究方向是数论。

目　　录

Contents

一　剩余类环的置换多项式



为简单起见，本章只讨论剩余类整数环 $Z/(m)$ 的置换多项式。对一般有单位元的交换环，如剩余类代数整数环，我们将不予考虑。值得指出的是，本章中的许多结果都可推广到有限域上去，这些将在第三章中加以介绍。

1. 从完全剩余系谈起

设 m 是一个正整数，从模 m 的每一个剩余类中选取一个代表元组成的集，称为模 m 的一个完全剩余系。例如 $\{0, 1, \cdots, m-1\}$ 组成模 m 的一个完全剩余系，$\{m+1, m+2, \cdots, 2m\}$ 也组成模 m 的一个完全剩余系。完全剩余系是数论中一个重要的基本概念，在高斯的名著《算术探讨》中就有系统研究。

我们所关心的问题是完全剩余系的构造，这就导致对置换多项式的研究。完全剩余系的最简单构造是 $\{b, a+b, 2a+b, \cdots, (m-1)a+b\}$，这里 a 是与 m 互素的一个整数。这个完全剩余系

可简单地用整系数线性多项式$ax+b$表示，也就是当x取值$0,1,\cdots,m-1$（模m的一个完全剩余系）时，$ax+b$正好就是所构造的完全剩余系。一般，自然要问哪些整系数多项式能够代表模m的完全剩余系？这便是本书的主题。

顺便指出，在大多数情形讨论整系数多项式代表完全剩余系的问题就足够了。事实上，后面将证明，当模m是一个素数时，模m的任一完全剩余系，甚至$Z/(m)$到$Z/(m)$的任一函数均可由某一整系数多项式表出。

定义 设$f(x)$是一整系数多项式。如果当x过模m的一个完全剩余系时，$f(x)$也过模m的一个完全剩余系，则称$f(x)$是模m的置换多项式。因为，此时$f(x)$正好导出$\{0,1,\cdots,m-1\}$的一个置换。

从$f(x+m)\equiv f(x)\pmod{m}$知，$f(x)$是模$m$的置换多项式相当于$\{f(0),f(1),\cdots,f(m-1)\}$是模$m$的一个完全剩余系。

因为模m的m个剩余类作成一个环，记为剩余类整数环$Z/(m)$，模m的置换多项式也可称为环$Z/(m)$的置换多项式。

定理1·1 设$f(x)$，$g(x)$是模m的两个置换多项式，$2\nmid m$，则$f(x)+g(x)$不是模m的置换多项式。

这个定理可从下述关于完全剩余系的引理直接得到。

引理1·2 [2] 设 $2 \mid m$，$\{a_1, \cdots, a_m\}$，$\{b_1, \cdots, b_m\}$是模m的两个完全剩余系，则$\{a_1+b_1, \cdots, a_m+b_m\}$不是模$m$的一个完全剩余系。

证 由假设

$$\sum_{j=1}^{m} a_j \equiv \sum_{j=1}^{m} j = \frac{m(m+1)}{2} \equiv \frac{m}{2} \pmod m$$

$$\sum_{j=1}^{m} b_j \equiv \sum_{j=1}^{m} j = \frac{m(m+1)}{2} \equiv \frac{m}{2} \pmod m$$

两式相加得

$$\sum_{j=1}^{m} (a_j + b_j) \equiv \frac{m}{2} + \frac{m}{2} \pmod m \quad (1.1)$$

另一方面，如果$\{a_1+b_1, \cdots, a_m+b_m\}$是模$m$的一个完全剩余系，则

$$\sum_{j=1}^{m} (a_j + b_j) \equiv \sum_{j=1}^{m} j = \frac{m(m+1)}{2} \equiv \frac{m}{2} \pmod m \quad (1.2)$$

这与（1.1）矛盾，因此$\{a_1+b_1, \cdots, a_m+b_m\}$不是模$m$的一个完全剩余系。□

注　当m为奇时，定理1·1一般不成立，例如取$f(x)=x$，$g(x)=2x$，$m=5$，则$f(x)$，$g(x)$是模5的置换多项式，而$f(x)+g(x)=3x$也是模5的置换多项式。

与引理1·2有关的一个概念是m元全差置换。设$(a_0 a_1 \cdots a_{m-1})$是$(0\ 1\ 2 \cdots (m-1))$的一个

置换，如果$\{a_0-0,\ a_1-1,\ a_2-2,\ \cdots,a_{m-1}-(m-1)\}$是模$m$的一个完全剩余系，则称置换$(a_0a_1\cdots a_{m-1})$是一个$m$元全差置换。以$N_0(m)$表示$m$元全差置换的个数，则引理1·2说明当$2\mid m$时，$N_0(m)=0$。当$m$是奇数时，设$m=2k+1$，令置换$\sigma=(2k\quad 2k-1\quad \cdots\quad k+1\quad k\quad k-1\quad \cdots\quad 1\quad 0)$，则因为$\{2k,\ 2k-2,2k-4,\cdots,2,\ 0,-2,\cdots,\ -2k\}$是模$m$的一个完全剩余系知$N_0(2k+1)>0$。因此，$N_0(m)>0$的充要条件是$m$为奇数·当$m\leqslant 15$时，$N_0(m)$的值已经算出，例如$N_0(13)=1030367$，$N_0(15)=36362925$，见〔4〕。

1968年，乔拉和查森豪斯〔13〕提出了下述两个猜想。

猜想Ⅰ 设f是一次数大于1的整系数多项式，p是一充分大的素数。若f是模p的置换多项式，则对所有$a\not\equiv 0 \pmod p$，$f(x)+ax$均不是模p的置换多项式。

猜想Ⅱ 设f是次数大于1的整系数多项式，p是充分大的素数。若f不是模p的置换多项式，则存在整数c，使得多项式$f(x)+c$是模p不可约的。

这两个猜想至今未被解决。

引理1·3 设n是m的一个正因子。若$f(x)$是模m的置换多项式，则$f(x)$也是模n的置换多项

式。

证 若$f(x)$不是模n的置换多项式，则当x过模n的完全剩余系时，$f(x)$不过模n的一个完全剩余系．因此有一整数a，使得$f(x)\equiv a \pmod{n}$无解。这样，$f(x)\equiv a \pmod{m}$也无解，从而$f(x)$不是模m的置换多项式，矛盾。□

对于两个置换多项式的乘积，现在可以证明

定理1·4 设$m>2$，$f(x)$，$g(x)$是模m的两个置换多项式，则乘积$f(x)\cdot g(x)$不是模m的置换多项式。

证 用反证法。设$f(x)\cdot g(x)$是模m的一个置换多项式，则$f(x)\cdot g(x)\equiv 0 \pmod{m}$只有一个解，因$f\equiv 0 \pmod{m}$，$g\equiv 0 \pmod{m}$各有一解，这两个解必须是相同的，经变换$x\longmapsto x+a$后，我们可不妨设$f(0)\equiv g(0)\equiv 0 \pmod{m}$。现分两种情况。

（i） 设有一奇素数$p\mid m$．由引理1·3知$f(x)$、$g(x)$、$f(x)\cdot g(x)$均是模p的置换多项式。设r是模p的一个原根，因$f(0)\equiv g(0)\equiv 0 \pmod{p}$，故存在整数$\{a_1, a_2, \cdots, a_{p-1}\}$，$\{b_1, b_2, \cdots, b_{p-1}\}$均作成模$(p-1)$的完全剩余系，满足

$$f(i)\equiv r^{a_i},\quad g(i)\equiv r^{b_i} \pmod{p}$$

对 $1\leqslant i\leqslant p-1$都成立。因此

$$f(i)g(i)\equiv r^{a_i+b_i} \pmod{p}\ (1\leqslant i\leqslant p-1)$$

从$f(0)\cdot g(0)\equiv 0 \pmod p$及$f(x)\cdot g(x)$是模$p$的置换多项式知$\{a_1+b_1, \cdots, a_{p-1}+b_{p-1}\}$必须是模$(p-1)$的一个完全剩余系。这与引理1·2矛盾。

(ii) $4\mid m$. 此时$f(x)$, $g(x)$, $f(x)\cdot g(x)$均是模4的置换多项式。直接验证知模4的两个完全剩余系的对应积不再是模4的完全剩余系。因此，$f(x)\cdot g(x)$不是模4的置换多项式。□

注 1948年，乔拉证明了更广泛的结果：模$m(m>2)$的两个完全剩余系的积不是模m的完全剩余系。另外，定理1·4还可推广到特征为奇的有限域上去，见第三章。

定理1·5 (i) 设$m=\prod_{i=1}^{k}p_i^{\alpha_i}$是$m$的标准分解式，则$f(x)$是模$m$的置换多项式当且仅当$f(x)$是模$p_i^{\alpha_i}(i=1, \cdots, k)$的置换多项式。

(ii) 设p是一素数，k是大于1的整数，则$f(x)$是模p^k的置换多项式当且仅当$f(x)$是模p的置换多项式，且导数$f'(x)\equiv 0 \pmod p$无解。

证 (i) 若$f(x)$是模m的置换多项式，则由引理1·3立得$f(x)$是模$p_i^{\alpha_i}(i=1, \cdots, k)$的置换式。反过来，若$f(x)$是模$p_i^{\alpha_i}(i=1, \cdots, k)$的置换多项式，如果$f(x)$不是模$m$的置换多项式，则存在整数$a_1\not\equiv a_2 \pmod m$使$f(a_1)\equiv f(a_2) \pmod m$。因$a_1\not\equiv a_2 \pmod m$，$p_i^{\alpha_i}(i=1,\cdots,k)$两两互素，有一$p_j$使$a_1\not\equiv a_2 \pmod{p_j^{\alpha_j}}$。而$f(a_1)$

$\equiv f(a_2)\pmod{p_i^{\alpha_i}}$，因此$f(x)$不是模$p_i^{\alpha_i}$的置换多项式，与假设矛盾。

(ii) 如果 $f'(x)\equiv 0\pmod p$无解且$f(x)$是模P的置换多项式，我们证明对每一整数a，同余式$f(x)\equiv a\pmod{p^k}$至多有一个解。我们先证$k=2$的情形，若此时有两个解x_1，x_2满足$x_1\not\equiv x_2\pmod{p^2}$，由$f(x_1)\equiv f(x_2)\pmod p$和$f(x)$是模p的置换多项式知$x_1\equiv x_2\pmod p$。设$x_1=x_2+pt$，则$f(x_1)=f(x_2+pt)\equiv f(x_2)+ptf'(x_2)\bmod p^2)$，故有$0\equiv f(x_1)-f(x_2)\equiv(x_1-x_2)f'(x_2)\pmod{p^2}$。因$f'(x_2)\not\equiv 0\pmod p$必有$x_1\equiv x_2\pmod{p^2}$，与所设矛盾．即$f(x)\equiv a\pmod{p^2}$至多有一个解。类似可证，$f(x)\equiv a\pmod{p^k}$至多有一个解。因$f(x)$取$p^k$个值（对应于$x$取0，1，…，$p^k-1$），故对每一$a$，$f(x)\equiv a\pmod{p^k}$恰有一解，这就是说$f(x)$是模$p^k$的置换多项式。

反过来，若$f'(x)\equiv 0\pmod p$有一解x_0，则$f(x_0+pi)\equiv f(x_0)+pif'(x_0)\pmod{p^2}\equiv f(x_0)\pmod{p^2}$，因此$f(x)\equiv f(x_0)\pmod{p^2}$至少有$p$个解$x=x_0+pi\ (i=0,1,\cdots,p-1)$，从而$f(x)$不是模$p^2$的置换多项式，当然更不是模$p^k$的置换多项式。

□

若多项式$f(x)$满足$f'(x)\equiv 0\pmod m$无解，则称f(x)是模m的正则多项式。定理1·5将模m

的置换多项式归结为模 p 的正则置换多项式。因此在以下几节中将重点讨论模 p 的置换多项式。因剩余类环 $Z/(p)$（也记为 F_p）是 p 个元的有限域，我们以后常称模 p 的置换多项式是有限域 F_p 的置换多项式，且同余式的语言用域中的等式运算来代替。

2. 置换多项式的判别与构造

置换多项式有下述几个等价的定义。

引理1·6 设 $f\in F_p[x]$，则 f 是 F_p 的置换多项式当且仅当以下条件之一成立。

(i) 函数 $f: c\longmapsto f(c)$ 是 F_p 到 F_p 的单射。

(ii) 函数 $f: c\longmapsto f(c)$ 是 F_p 到 F_p 的满射。

(iii) 对任何 $a\in F_p$，$f(x)=a$ 在 F_p 中有解。

(iv) 对任何 $a\in F_p$，$f(x)=a$ 在 F_p 中有唯一解。

证 (i)$\longrightarrow$(ii)，因 F_p 只含有限个元（p 个元），故单射是满射。

(ii)$\longrightarrow$(iii) (iii)是(ii)的另一种说法。

(iii)$\longrightarrow$(iv) 因 F_p 只有有限个元，$f(x)$ 必须是 F_p 到 F_p 的单射，故(iv)成立。

(iv)$\longrightarrow$(i) (i)是(iv)的直得推论。

(iv)和置换多项式的定义等价。

有限域F_p到自身的任一函数均可由$F_p[x]$中的多项式表出。事实上，设$\phi(x)$是F_p到F_p的任一函数，令

$$g(x)=\sum_{c\in F_p}\phi(c)\left(1-(x-c)^{p-1}\right) \quad (1.3)$$

直接验证知$g(b)=\phi(b)$对所有$b\in F_p$成立，且$g(x)$的次数$<p$。因此$\phi(x)$可由$F_p[x]$中次数小于p的多项式表出。

设$f(x)\in F_p[x]$，由欧几里得算法知，存在$F_p[x]$中次数小于p的多项式$g(x)$使得

$$f(x)\equiv g(x)\ (\bmod\ (x^p-x))$$

因x^p-x在F_p上恒取零值，故$g(c)=f(c)$对所有$c\in F_p$成立。这样，$F_p[x]$中任一多项式$f(x)$经模(x^p-x)后均可化为一次数小于p的多项式$g(x)$，$g(c)=f(c)$对所有$c\in F_p$均成立。$g(x)$称为$f(x)$模(x^p-x)的简化多项式，$g(x)$的次数$\deg(g(x))$称为$f(x)$的简化次数。

引理1·7 设f，$f_1\in F_p[x]$，则$f(c)=f_1(c)$对所有$c\in F_p$成立当且仅当$f(x)\equiv f_1(x)\ (\bmod (x^p-x))$。

证 由欧几里得算法，存在次数小于p的多项式$r(x)$满足

$$f(x)-f_1(x)\equiv r(x)\ (\bmod (x^p-x))$$

因为$f(c)=f_1(c)$，$c^p-c=0$对所有$c\in F_p$成立，

故$r(c)=0$。对所有$c\in F_p$成立。从$r(x)$的次数小于p知，$r(x)$是零多项式，即$f(x)\equiv f_1(x) \pmod{(x^p-x)}$。上述证明反过来也成立。□

引理7·1 说明简化多项式是被唯一确定的，简化次数因而也被唯一确定。

定理1·8 设$f\in F_p[x]$，则f是F_p的置换多项式当且仅当下面两个条件成立。

(i) f在F_p中恰有一个零点。

(ii) 对每一整数t，$1\leqslant t\leqslant p-2$，$f(x)^t$模$(x^p-x)$的简化次数不超过$p-2$。

这个定理是关于置换多项式的最早的结果，它是由厄米特在1863年证明的。1896年，迪克逊将该定理推广到有限域上。1970年，格温伯格给出了一个新证明。1978年[11]，卡里兹和路兹又给出了一个新证明。在第三章，我们将给出另一个证明。

注 1891年，罗格尔曾将定理1·8中的条件$1\leqslant t\leqslant p-2$改进为$1\leqslant t\leqslant\frac{p-1}{2}$。但此结果不能推广到一般的有限域上去。

定理1·8的另一种形式为

定理1·9 设$f\in F_p[x]$，则f是F_p的置换多项式当且仅当下面两个条件成立。

(i) $f(x)^{p-1}$的简化次数是$p-1$。

(ii) $f(x)^t$ $(1\leqslant t\leqslant p-2)$ 的简化次数不超

过$(p-2)$。

上述两个定理的证明可在第三章中找到，在那里，结果还要广泛些。

定理1·8，定理1·9有时可用来判别$F_p(x)$中的多项式是不是F_p的置换多项式，故定理1·8（或定理1·9）有时又称为厄米特判别法（准则）．下面我们举两个例子来说明厄米特准则在判别置换多项式时的应用。

定理1·10 设r是正整数，$(r, p-1)=1$，s是$(p-1)$的一个正因子。再设$g(x)\in F_p[x]$，满足$g(x^s)$在F_p中无非零根。则多项式

$$f(x)=x^r(g(x^s))^{\frac{p-1}{s}}$$

是F_p的置换多项式。

证 我们用定理1·8来证这个结果。条件(i)显然是满足的。为证(ii)，取$t\in Z$，$1\leqslant t\leqslant p-2$。

先设$s\nmid t$。此时$f(x)^t$的展开式中x的方幂为形如$rt+ms$的整数，其中m是非负整数。因$s\nmid t$，则$s\nmid rt+ms$，从而$(p-1)\nmid rt+ms$。于是$f(x)^t$模(x^p-x)的简化次数不超过$(p-2)$（这是因为$(p-1)\nmid rt+ms$，故x^{rt+ms}模(x^p-x)后不能是x^{p-1}这一项）。

再设$t=ks$，k是正整数。此时

$$f(x)^t = x^{rt}(g(x^s))^{(p-1)k}$$

令$h(x) = x^{rt}$，则有$f(c)^t = h(c)$对所有$c \in F_p$成立，因为当$c \neq 0$时，$g(c^s) \neq 0$。再由引理1·7得

$$f(x)^t \equiv h(x) = x^{rt} (\mathrm{mod}(x^p - x))$$

而$(p-1) \nmid rt$，故$f(x)^t$的简化次数不超过$p-2$。

综上，应用定理1·8即得。□

定理1·11 设$1 < k < p$。如果

(i) $p-1 > (k-1)(k-1, p-1)$,

或

(ii) $p-1 \geqslant k[(k-1, p-1)-1] > 0$,

成立，则$f(x) = x^k + ax(a \neq 0)$不是$F_p$的置换多项式。

定理1·11可借助于定理1.8来证明，见[7]。一般，可用深入的兰—魏依定理来证明$f(x) = x^k + ax(a \neq 0)$在$p > 0(k^4)$时，不是$F_p$的置换多项式。这个结果可推广到任意有限域上去。而定理1·11是否可推广到任意有限域上去，仍值得研究。

3. 迪克逊多项式

本节中，我们介绍一类很重要的置换多项式，即迪克逊多项式。

设k是正整数，x_1，x_2为变元，由附录中的

华林公式得恒等式

$$x_1^k + x_2^k = \sum_{j=0}^{\left[\frac{k}{2}\right]} \frac{k}{k-j}\binom{k-j}{j}(-x_1x_2)^j (x_1+x_2)^{k-2j} \tag{1.4}$$

定义迪克逊多项式如下：

$$g_k(x,\ a) = \sum_{j=0}^{\left[\frac{k}{2}\right]} \frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j} \tag{1.5}$$

上式中方括号“$[b]$”表示实数 b 的整数部分。$g_k(x,\ a)$称为迪克逊多项式。它和分析中的第一类切比雪夫多项式有密切联系，因此在有些文献中又称为切比雪夫多项式。

在(1.4)中令 $x_1 = y$，$x_2 = \frac{a}{y}$得

$$g_k\left(y+\frac{a}{y},\ a\right) = y^k + \left(\frac{a}{y}\right)^k \tag{1.6}$$

特别，当$a=0$时有

$$g_k(x,\ 0) = x^k \tag{1.7}$$

x^k是F_p的置换多项式当且仅当$x_1^k \neq x_2^k$ ($x_1 \neq x_2 \in F_p$)，即$\left(\frac{x_1}{x_2}\right)^k \neq 1$。由附录知$x^k = 1$在$F_p$中的解数为$(k,\ p-1)$。因此$g_k(x,\ 0) = x^k$是$F_p$的置

换多项式当且仅当$(k, p-1)=1$。

当$a\neq 0$时，有下述

定理1·12 设$a\neq 0$，$a\in F_p$。则由迪克逊多项式$g_k(x, a)$是F_p的置换多项式当且仅当$(k, p^2-1)=1$。$g_k(x, a)$是F_p的正则置换多项式当且仅当$(k, p(p^2-1))=1$。

证 设$(k, p^2-1)=1$。若有b，$c\in F_p$使得$g_k(b, a)=g_k(c, a)$，我们来推出$b=c$。在F_p的某一个二次扩域中取一非零元β使$\beta+a\beta^{-1}=b$，同样又在F_p的另一个二次扩域中取一非零元γ使$\gamma+a\gamma^{-1}=c$。因F_p的所有二次扩域都是同构的，β和γ都可在F_p的同一个二次扩域F_{p^2}中选取。由(1.6)有

$$g_k(b, a)=\beta^k+\left(\frac{a}{\beta}\right)^k$$

$$=\gamma^k+\left(\frac{a}{\gamma}\right)^k=g_k(c, a)$$

因此$(\beta^k-\gamma^k)(\beta^k\gamma^k-a^k)=0$。由此有$\beta^k=\gamma^k$或$\beta^k=(a\gamma^{-1})^k$。因$(k, p^2-1)=1$，故又有$\beta=\gamma$，或$\beta=a\gamma^{-1}$。无论在什么情况下，都有$b=c$。即$g_k(x, a)$是$F_p$的置换多项式。

再设$(k, p^2-1)=d>1$。若$2|d$，则$2|k$，$2\nmid p$。(1.5)表明$g_k(x,a)$只含x的偶数次方幂，因此对所有$c\in F_p^*$有$g_k(c,a)=g_k(-c,a)$。而$c\neq$

$-c$，故$g_k(x,a)$不是F_p的置换多项式．下设$2\nmid d$，则有 d 的奇素因子 r，$r|k$，$r|(p-1)$或$r|(p+1)$．分两种情况．当$r|(p-1)$时，方程$x^r=1$在 F_p中有 r个解，因此存在$b\in F_p^*$，$b^r=1$，$b\neq 1$，a．于是$b^k=1$，且由(1.6)得

$$g_k(b+ab^{-1},\ a)=1+a^k=g_k(1+a,\ a)$$

因$b\neq 1$，a，故$b+ab^{-1}\neq 1+a$，这样 $g_k(x,\ a)$就不是 F_p 的置换多项式．当 $r|(p+1)$时，设 γ 是F_p的二次扩域F_{p^2}中的一元使得$\gamma^{p+1}=a$．因$x^r=1$在 F_{p^2}中有 r 个解，于是存在 $\beta\in F_{p^2}$，$\beta^r=1$，$\beta\neq 1$，$a\gamma^{-2}$．这样就有$\beta^{p+1}=1$，$\beta^k=1$且

$$g_k(\gamma+a\gamma^{-1},a)=g_k(\beta\gamma+a(\beta\gamma)^{-1},a)$$

因为，F_{p^2}中x^p-x的所有零点组成F_p，故有$\gamma+a\gamma^{-1}=\gamma+\gamma^p\in F_p$，$\beta\gamma+a(\beta\gamma)^{-1}=\beta\gamma+(\beta\gamma)^p\in F_p$．因$\beta\neq 1$，$a\gamma^{-2}$，我们推得$\gamma+a\gamma^{-1}\neq\beta\gamma+(\beta\gamma)^{-1}$，因此$g_k(x,\ a)$不是$F_p$的置换多项式．

下面证明定理的第二部分．从(1.6)得

$$g_k(x+a/x,\ a)=x^k+\left(\frac{a}{x}\right)^k$$

对 x 求导得

$$g_k'(x+\frac{a}{x},\ a)(1-\frac{a}{x^2})$$

$$=kx^{k-1}-k\frac{a^k}{x^{k+1}} \tag{1.8}$$

因此有

$$g_k'(x+\frac{a}{x}, a)=k\frac{(x^2)^k-a^k}{x^{k-1}(x^2-a)}$$

$$=\frac{k}{x^{k-1}}\sum_{j=0}^{k-1}(x^2)^{k-1-j}a^j$$

$$=\frac{k}{x^{k-1}}h(x), \quad h(x)\in Z[x] \qquad (1.9)$$

如果 $g_k(x, a)$是 F_p 的正则置换多项式，则有 $g_k'(x, a)$在F_p中无零点。从(1.9)得出，$p\nmid k$，综定理的第一部分得$(k, p(p^2-1))=1$。

反过来，设$(k,p(p^2-1))=1$。若有$s\in F_p$，使$g_k'(s, a)=0$，在F_p的某二次扩域中取一元$u\neq 0$使$u+\frac{a}{u}=s$，代入(1.9)得$h(u)=0$。于是有

$$(u^2-a)h(u)=(u^2)^k-a^k=0$$

从$(k, p^2-1)=1$得$u^2=a$，因此有

$$h(u)=\sum_{j=0}^{k-1}(u^2)^{k-1-j}a^j=\sum_{j=0}^{k-1}a^{k-1}$$

$$=ka^{k-1}=0$$

必有$p|k$，矛盾。故$g_k(x, a)$是F_p的正则置换多项式。

定理全部证完。

定理1·12本质上是由迪克逊在1897年证明

的。1968年，诺鲍尔给出了一个完全的证明。1971年，威廉斯用另一种方法证明了定理1·12的充分性部分。

由于在公开密钥码中的应用，下面我们来讨论由迪克逊多项式作成的群。

定义 设$f(x)$，$g(x)$是$F_p[x]$中的两个多项式，称多项式$f(g(x))$为f与g的合成。

从置换多项式的定义看出，两个置换多项式的合成仍然是一置换多项式。由于合成运算还满足结合律，因此，F_p的所有置换多项式在合成运算下作一群。这个群的进一步研究将在第三章中给出。对于迪克逊多项式，它们是否能作成一个子群呢？

定义两个多项式类如下：

$$P(0)=\{g_k(x,\ 0)\mid k\in Z^+,(k,\ p-1)=1\}$$

$$P(a)=\{g_k(x,a)\mid k\in Z^+,\ (k,\ p^2-1)=1\}$$

上式中Z^+表示由全体正整数组成的集合，a是F_p中的非零元。$P(0)$，$P(a)$均是由置换多项式组成的集合。

定理1·13 $P(a)$在多项式的合成运算下是封闭的当且仅当$a=0$，± 1，且此时还有关系$g_{km}(x,\ a)=g_k(g_m(x,\ a),a)$，因此$P(a)$是由$F_p$的

置换多项式作成的一个交换群（阿贝尔群）。

证 设$a\in F_p$，k，$m\in Z^+$，则

$$g_k\left(g_m(y+\frac{a}{y},a),a^m\right)$$

$$=g_k(y^m+\frac{a^m}{y^m},\ a^m)$$

$$=y^{km}+\frac{a^{km}}{y^{km}}$$

$$=g_{km}\left(y+\frac{a}{y},\ a\right)$$

由(1.6)得

$$g_{km}(x,\ a)=g_k(g_m(x,\ a),\ a^m)\quad(1.10)$$

如果$P(a)$在合成运算下是封闭的，则有$g_k(g_m(x,a),a)$在$P(a)$中，比较x的次数得

$$g_k(g_m(x,\ a),\ a)=g_{km}(x,\ a)$$

再由(1.10)知

$$g_k(g_m(x,\ a),a)=g_k(g_m(x,\ a),\ a^m)$$

因$g_m(x,\ a)$不是常数，故又有

$$g_k(x,\ a^m)=g_k(x,\ a)$$

当$k>1$时，比较x^{k-2}的系数得

$$a^m=a$$

如果$a\neq 0$，因$g_m(x,\ a)\in P(a)$，则$(m,\ p^2-1)=1$，再从$a^m=a$得$a=\pm 1$。

反过来，若$a=0$，± 1，由上述过程直接验

证知$P(a)$在合成运算下是封闭的。□

上述定理表明，当$a=0$，± 1时，$P(a)$作成一交换群。

4. 置换谱

设$f(x)$是一个整系数多项式。前面考虑了对给定的整数m（特别是素数p），$f(x)$是不是模m的置换多式项.这是一个局部性的问题.本节考虑一个涉及整体性的问题，即在所有的整数中，$f(x)$能是哪些整数模m的置换多项式，即决定下列集合

$M(f)=\{m|m\in Z^+$，f 是模m的置换多项式$\}$

$M(f)$ 称为多项式f的置换谱，它是由诺鲍尔于1965年首先提出并加以研究的，见〔36〕。

定理1·5说明集合$M(f)$可以归结为下列两个由素数组成的集合：

$S(f)=\{p|$ p是素数，f是模p的正则置换多项式$\}$

$T(f)=\{p|p$是素数，f是模p的置换多项式，但非正则的$\}$

由定理1·5，集合$M(f)$可由下面的定理给出：

定理1·14　置换谱

$$M(f)=\{p_1\cdots p_r q_1^{a_1}\cdots q_s^{a_s}\,|\,p_i\in T(f),\ q_j\in S(f),\ a_j\geqslant 1\}$$

我们所关心的问题之一是决定置换谱 $M(f)$ 中素数的个数，这个数就是集合

$$P(f)=S(f)\cup T(f) \qquad (1.11)$$
$$=\{p\,|\,p\text{是素数，}f\text{是模}p\text{的置换多项式}\}$$

中元素的个数。本节中我们将给出$P(f)$是无限集的充分必要条件。

引理1·15 设 f 是整系数多项式 f_1，…，f_n 的合成，则有

$$M(f)=M(f_1)\cap M(f_2)\cap\cdots\cap M(f_n) \qquad (1.12)$$

$$S(f)=S(f_1)\cap S(f_2)\cap\cdots\cap S(f_n) \qquad (1.13)$$

$$P(f)=P(f_1)\cap P(f_2)\cap\cdots\cap P(f_n) \qquad (1.14)$$

证 据数学归纳法，只需证明引理1.15对 $n=2$成立。于是可不妨设$f=f_2(f_1)$。

首先，由置换多项式的定义及多项式合成运算的定义知，f 是模m的置换多项式当且仅当 f_1和 f_2 均是模m的置换多项式。由这个性质立即推出(1.12)和(1.14)成立。

其次，根据复合函数的求导运算知

$$f'(x)=f_2'(f_1(x))\cdot f_1'(x)$$

于是

$$f'(x)\equiv 0 \pmod p$$

无解当且仅当

$$f_1'(x)\equiv 0 \pmod p$$

$$f_2'(y)\equiv 0 \pmod p$$

均无解。这就是说 $f(x)$ 是模 p 的正则多项式当且仅当$f_1(x)$，$f_2(x)$均为模 p 的正则多项式。结合(1.14)知(1.13)成立。□

设 H 是由线性多项式 $ax+b(a\neq 0)$，方幂 $x^n(2\nmid n,\ n>1)$和迪克逊多项式$g_n(x,\ a)(a\neq 0,\ (n,\ 6)=1,\ n>1)$所生成的多项式集（运算是多项式的合成运算）。在这个运算下，H显然作成一群。又设L是由H中由线性多项式$ax+b$和迪克逊多项式$g_n(x,\ a)$所生成的H的子群。则有

定理1·16 如果 $f\in H$，则$P(f)$是无限集。进一步，在$f\in H$的条件下，还有$S(f)$是无限集当且仅当$f\in L$。

证 显然有

$$P(ax+b)=\{p\,|\,a\not\equiv 0 \pmod p\}$$

$$P(x^n)=\{p\,|\,(n,\ p-1)=1\}$$

由定理1·12还有

$$P(g_n(x,\ a))=\{p\,|\,a\not\equiv 0 \pmod p,\ (n,\ p^2-1)=1\}\cup\{p\,|\,a\equiv 0 \pmod p,$$

$(n, p-1)=1\}$

如果$n=r_1^{e_1}\cdots r_s^{e_s}$是 n 的标准分解式，则

$$P(x^n)=\{p|p\not\equiv 1(\bmod\ r_i), i=1,\cdots, s\}$$

$$P(g_n(x, a))=\{p|a\not\equiv 0(\bmod p),$$

$$p\not\equiv \pm 1(\bmod\ r_i),\ i=1,\cdots,s\}\cup\{p|a$$

$$\equiv 0(\bmod p), p\not\equiv 1(\bmod\ r_i), i=1,\cdots,s\}$$

现设 $f\in H$。则 f 是f_1，…，f_t 的合成，其中f_i等于$ax+b$，或者$x^n(2\nmid n)$，或者 $g_n(x, a)$ $((n,6)=1, a\neq 0, n>1)$。又设 f 的次数$\deg(f)=u_1^{e_1}\cdots u_s^{e_s}v_1^{d_1}\cdots v_r^{d_r}$ 是其标准分解式，其中每一u_i均整除某一形如x^n的f_i的次数，但不整除任一形如$g_n(x,a)$的f_i的次数，v_i是剩下的$\deg(f)$的素因子。记

$$\overline{P}(f)=\{p|p\not\equiv 1(\bmod\ u_i)(i=1,\cdots,s),$$
$$p\not\equiv \pm 1(\bmod\ v_j)(j=1,\cdots,r)\}$$

由前面关于集合$P(f)$的讨论知，$P(f)$和 $\overline{P}(f)$仅差有限个素数，也就是说$P(f)$可用 $\overline{P}(f)$ 经移去或加入有限个素数来得到。由假设$u_i\neq 2(i=1,\cdots,s)$，$v_j\neq 2,3$ $(j=1,\cdots,r)$。因此 $P(\overline{f})$ 的素数由模$u_1\cdots u_sv_1\cdots v_r$的$(u_1-1)\cdots(u_s-1)(v_1-2)\cdots(v_r-2)$个剩余类中的全体素数组成，其中正好有$(u_1-2)\cdots(u_s-2)(v_1-3)\cdots(v_r-3)(>0)$个剩

余类与模$u_1\cdots u_s v_1\cdots u_r$互素。由算术级数的狄里克雷定理知，每一个这样的互素剩余类中都有无限个素数。因此$\overline{P}(f)$是无限集，从而$P(f)$是无限集。定理的前一部分得证。

现证后一部分。因为当$n>1$时，$S(x^n)=\phi$（即空集）。故若$f\in H-L$，由引理1·15有$S(f)=\phi$，当然为有限集。又若$f\in L$，则$f\in H$，因此$P(f)$是无限的。现只需证明$P(f)-S(f)$为有限集。由定义有

$$S(ax+b)=P(ax+b)$$

又从定理1·12得

$$S(g_n(x,\ a))=\{p\,|\,a\not\equiv 0(\mathrm{mod}\ p),\ (n,\ p(p^2-1)=1)\}$$
$$=\{p\,|\,p\in P(g_n(x,\ a)),\ a\not\equiv 0(\mathrm{mod}\ p),\ p\nmid n\}$$

由这个式子看出$P(f)-S(f)$是有限集，因此$S(f)$是无限集。

至此定理全部证完。

定理1·16给出了使$P(f)$是无限集的一类多项式。那么是否还存在另外的多项式$f(x)$使$P(f)$也为无限集呢？1923年[40]，舒尔提出了下述著名的猜想，即

舒尔猜想 $P(f)$是无限集当且仅当$f\in H$；

$S(f)$是无限集当且仅当 $f \in L$。

如果这个猜想的前一部分成立，由定理1·16知该猜想的后一部分也成立。因此只需证明猜想的前一部分成立。

1923年[40]，舒尔本人证明当deg(f)是素数时，上述猜想成立。

1928年[42]，威格纳证明当deg(f)是奇素数幂或两个奇素数的积时，舒尔猜想成立。

1947年[20]，库尔巴托夫证明当 deg$(f)=p_1\cdots p_k$，p_i是不同的奇素数，任一p_i不能表成其余p_i的非负整线性组合时，舒尔猜想成立。

1949年[21]，库尔巴托夫又证明当deg(f)是至多 4 个不同奇素数的积或两个不同奇素数的幂的积时，舒尔猜想成立。

1970年[17]，弗雷德用黎曼曲面理论中的深入工具完全解决了舒尔猜想。

利用弗雷德的深刻结果，可以得到很多有趣的推论。例如，结合弗雷德的结果和定理1·16的证明有下述两个推论。

推论1·17 如果$P(f)$是无限集，则$S(f)$是空集或是无限集。

推论1·18 若$P(f)$是无限集，则$P(f)$和下面的素数集$\overline{P}$仅差有限个素数。这里$\overline{P}$的形式为

$$\overline{P}=\{p \mid p \equiv b(\bmod u_1\cdots u_s v_1\cdots v_r),$$

$b \neq \pm 1 \pmod{v_i}, b \neq 1 \pmod{u_j}$,
$v_i \neq 2, 3, u_j \neq 2, u_i, v_j$ 为不同的素数}

利用弗雷德的结果，还可证明下述达文波特和刘易斯的定理，见〔15〕。

定理1·19 设 $f \in Z[x]$。如果 f 的次数 $\deg(f)$ 是偶数（>0），则 $P(f)$ 是有限集。

证 用反证法。假设 $P(f)$ 是无限集，则由弗雷德的结果知 $f \in H$。即 f 由 $f_1, \cdots, f_t$ 合成，其中 $f_i = ax+b$，x^n $(2\nmid n, n>1)$ 或迪克逊多项式 $g_n(x, a)$ $(a\neq 0, (6, n)=1, n>1)$，于是 $\deg(f_i)$ 全部是奇数。从

$$\deg(f) = \deg(f_1)\cdot\deg(f_2)\cdot\cdots\cdot\deg(f_t)$$

得知 $\deg(f)$ 也为奇数，这与定理的假设矛盾。□

弗雷德的结果还可用来证明诺鲍尔的一个定理

定理1·20 设 S，T 是两个不相交的有限的素数集，则存在无限多个多项式 $f \in Z[x]$ 使 $S(f) = S$，$T(f) = T$。

证 如果 $S\cup T$ 是空集。取 $f(x) = 2x^{2^n}$ 就行了。现假设 $S\cup T$ 是非空集，q 是大于 $S\cup T$ 中所有素数的一个素数。对 $S\cup T\cup\{q\}$ 中的每一素数 p，定义多项式

$$f_p(x)=\begin{cases}x, & 若p\in S,\\ x^{a_p}, & 若p\in T,\\ x^{2a}, & 若p=q.\end{cases}$$

其中a_p是与$p(p-1)$互素的任一素数，a是大于所有$1+a_p$的任一整数。由多项式环中的孙子定理，存在一次数为$2a$的整系数多项式$f_0(x)$使

$$f_0(x)\equiv f_p(x)\pmod{p}$$

对所有$p\in S\cup T\cup\{q\}$均成立。从$f_0(x)$的构造知，当$p\in S$时，$p\in S(f_0)$；当$p\in T$时，有$p\in T(f_0)$。因此$S(f_0)\geqslant S$，$T(f_0)\geqslant T$，由达文波特—刘易斯定理知$P(f_0)$是有限的。令D是$P(f_0)-S\cup T$中所有素数的积，并设

$$f(x)=Df_0(x)$$

则有

$$S(f)=S,\quad T(f)=T.$$

因次数$2a$可以取得任意大，故有次数任意大的多项式$f(x)$满足定理的要求。□

二 置换多项式的应用举例

置换多项式有许多应用。本节只介绍置换多项式在公开密钥码和一致分布中的应用。在这里，可看出迪克逊多项式的重要性。

1 .密码系统简介

大家知道，密码通讯在许多部门都起着极为重要的作用，那么密码通讯究竟是以什么方式进行的呢？本节就是以简单的例子来说明密码通讯的基本原理。

通讯就是发送或接收信息。在发送信息时，需要先将被发送的信息转换成数字.例如，在英文里共有26个字母，可以设$a=0$，$b=1$，$c=2$，…$x=23$，$y=24$，$z=25$。这样，信息（可用语言表示）便可被转换成一组相应的数字。在实际过程中，可能还要使用空格，标点符号，及其它一些符号，这时可将上述字母与数字的对应关系继续扩大，如可以设“空格”=26，标点“，”=27，标点“？”=28，…。为简单起见，我们只

讨论由26个英文字母组成的信息.

上面已指出，信息可看成是一组数字，因此对信息加密的问题就化为对数字编码的问题。

最简单的编码方法是将26个字母放在圆周上，每一个字母经编码后变成它后面的一个字母。用对应的数字来说，编码就是同余式

$$C \equiv P + 1 \pmod{26}, \quad 0 \leqslant C \leqslant 25 \qquad (2.1)$$

其中P对应于要发送的字母，C对应于编码后的字母。

例如，假设要发送的信息是

secret.

首先将这几个字母转换成对应的数字得到

18　4　2　17　4　19

用（2.1）编码后得

19　5　3　18　5　20

再转换成对应的字母得

tfdsfu.

这就是信息“*secret*”的密文。

当发送的信息是很长一串字母时，可将该串分成若干段进行.

注意，知道了编码过程（2.1），也就知道了解码过程。事实上，从（2.1）得

$$P \equiv C - 1 \pmod{26}. \qquad (2.2)$$

因此一旦收到了一组从（2.1）加密后的密文，用（2.2）就可解开这个密码。

上述例子只是非常简单的一个情形。在实际的密码通讯系统中，要复杂得多。尽管如此，密码系统的基本原理均可概述如下：

假设发送信息的一方为S，接收信息的一方为R，收方有解密密钥D_R，发方有加密密钥E_R。这两个密钥是互逆的，即有

$$D_R \cdot E_R = E_R \cdot D_R = 1$$

假设要发送一个秘密信息M。发方S将M用E_R加密得到$E_R(M)$，然后将此密文发出。收方R收到密文$E_R(M)$后，用解密密钥D_R于密文$E_R(M)$上即得

$$D_R \cdot (E_R(M)) = D_R \cdot E_R(M) = M$$

这样就获得了原始信息M。

在传统的保密系统中，只要知道一个密钥，另一个密钥就可很容易地导出来。因此，为使发送的密码信息不被第三者破译，必须严格保密两个密钥D_R，E_R。这样，由于每两方都有一对保密的密钥，当系统中用户较多时，密钥数量就很大，难以分配和管理。为避免这一缺陷，1978年[39]，里维斯特，夏米尔，阿德利曼构造出了一种新的保密系统。在这种系统中，由于从加密密钥E_R几乎不能导出解密密钥D_R，因此，加密密

钥E_R都是公开的，这种非常重要的系统称为RSA系统。

在RSA系统中，其工作原理如下：系统中的每一方均有一对互逆的密钥（E_R，D_R），其中仅有解密密钥是保密的。加密密钥E_R全部被收集在一个密码簿内，供系统中的任何一方查阅。假设发方S要把信息M发给收方R。S先在密码簿内查出R方的加密密钥E_R，用E_R加密M得到$E_R(M)$，然后将密文$E_R(M)$发给收方R。R收到$E_R(M)$后，用自己的解密密钥D_R于密文$E_R(M)$上得

$$D_R\cdot(E_R(M))=D_R\cdot E_R(M)=M$$

即获得了发方S的原始信息。因为从E_R几乎不可能导出D_R，故第三者无法破译密文$E_R(M)$。这就保证了RSA系统的可行性。

在下面两节中，将说明如何用置换多项式来构造RSA系统。从这种观点出发，可以看出置换多项式是研究RSA系统的构造的一个理想工具。

2．迪克逊多项式与RSA系统

在RSA系统中，加密密钥E_R相当于一个数集A的置换，而解密密钥D_R则相当于置换E_R的逆置换。当A是剩余类环$Z/(m)$时，这些置换可取为模m的置换多项式。里维斯特，夏米尔和

阿德利曼所取的模m的置换多项式为x^k，$(k, \varphi(m))=1$。$m=pq$，p，q是不同的大素数。设k_1是一正整数，满足

$$kk_1 \equiv 1 (\bmod\ \varphi(m))$$

则当$(M, m)=1$时，有

$$(M^k)^{k_1}=M^{kk_1}\equiv M(\bmod m) \quad (2.3)$$

因$m=pq$无平方因子，当$(M, m)>1$时(2.3)仍然成立。这样可取加密密钥为x^k，解密密钥为x^{k_1}.在这个系统中，只有k和m是公开的。要求得解密密钥，即求出k_1，必须先求出

$$\varphi(m)=(p-1)(q-1)=m-p-q+1$$

但是p，q只能从分解m才能得到。由于p，q是保密的大素数，要分解$m=pq$几乎是不可能的。正是分解大整数的困难性保证了RSA系统的可靠性。

多项式簇$\{x^k|k=1,2,\cdots\}$有下面一些性质：

(i)在多项式的合成运算下，$\{x^k\}$作成一个阿贝尔群(即交换群)。$x^k \circ x^l=x^{kl}=x^l \circ x^k$。

(ii)对每一正整数k，$(k,\varphi(m))=1$，存在正整数k_1，使得$x^k \circ x^{k_1}=x^{k_1} \circ x^k$是模$m$的单位置换多项式，即该置换多项式可等价地化为$x$（单位置换多项式）。

(iii)给定一个正整数k，满足$(k,\varphi(m))=1$，很难求得k_1使$x^k \circ x^{k_1}=x^{kk_1}$是模$m$的单位置换

多项式。

上述三个性质保证了多项式簇$\{x^k|k=1,2,\cdots\}$能够构造出一个RSA系统。

注意，多项式簇$\{x^k|k=1,2,\cdots\}$正是当$a=0$时的迪克逊多项式簇$\{g_k(x,a)|k=1,2,\cdots\}$。米勒和诺鲍尔[32]于是建议用迪克逊多项式簇$P(a)=\{g_k(x,a)|k=1,2,\cdots\}(a=\pm1)$来代替多项式簇$\{x^k\}=\{g_k(x,0)\}$，以构造一种新的RSA系统。

在第一章的第三节中，定义了迪克逊多项式为

$$g_k(x,a)=\sum_{i=0}^{[\frac{k}{2}]}\frac{k}{k-i}\binom{k-i}{i}(-a)^i x^{k-2i}$$

在那里已经证明，当$a=\pm1$时，多项式簇$\{g_k(x,a)\}$作成一阿贝尔群，且满足

$$g_k(x,a)\circ g_n(x,a)=g_{kn}(x,a)$$

即条件(i)满足。

当$a=1$时，$g_k(x,1)=g_k$的递归关系为

$$g_{k+2}-xg_{k+1}+g_k=0,\quad g_0=2,\quad g_1=x$$

因此，g_k可用上述递归关系来计算。

如果$m=pq$，p，q是不同的素数，则第一章的第三节已证明，$g_k(x,a)$是模m的置换多项式当且仅当

$$(k,\ (p^2-1)(q^2-1))=1$$

进一步，劳斯基，米勒和诺鲍尔[23] 证明$g_{k_1}(x,a)$是$g_k(x,a)$的逆当且仅当

$$kk_1 \equiv 1(\mathrm{mod}(p^2-1)(q^2-1)) \qquad (2.4)$$

即条件(ii)满足。

从 (2.4) 看出，如果仅知道k和m，要求出k_1几乎是不可能的，因为仍然要分解大整数。因此条件(iii)也成立。

这样，和多项式簇$\{x^k\}=\{g_k(x,0)\}$一样，迪克逊多项式簇$\{g_k(x,1)\}$和$\{g_k(x,-1)\}$也可用来构造新的RSA系统。

利用劳斯基和诺鲍尔关于置换链的一个结果，可以证明，三类迪克逊多项式簇$\{g_k(x,a)\}$ $(a=0,\pm1)$在本质上给出了所有满足下列条件的多项式类：

1）对任何正整数k，在这个类中存在一次数为k的多项式。

2）该类中的任何两个多项式在合成运算下是可换的，即$f(g)=g(f)$成立。

这样，由构造RSA系统的多项式类所具有的性质知，三类迪克逊多项式$\{g_k(x,a)\}$ $(a=0,\pm1)$在某种意义上给出了所有构造RSA系统的多项式类。

上述RSA系统的构造方法可推广到多变元的

多项式类上，这时多变元迪克逊多项式仍起着决定性的作用。

3. 置换有理函数与RSA系统

前节中考虑了由置换多项式构造的RSA系统。作为置换多项式的进一步应用，本节再考虑由更广泛一些的置换有理函数所构造的RSA系统。

设$r(x)=\dfrac{g(x)}{h(x)}$是两个整系数多项式的商，其中g，h在$Z[x]$中是互素的多项式。如果对任何$b\in Z$有$(h(b),m)=1$，并且映射

$$\pi:\ Z/(m)\to Z/(m)$$
$$\pi(b)=h(b)^{-1}g(b)$$

是模m的一个置换，则称$r(x)$为模m的置换有理函数。这个概念是置换多项式的推广。多项式$g(x)$是模m的置换多项式当且仅当$g(x)/1$是模m的置换有理函数。如果$m=m_1m_2$，$(m_1,m_2)=1$，则易证$r(x)$是模m的置换有理函数当且仅当$r(x)$是模m_1和模m_2的置换有理函数。

1946年[38]，里德研究了有限域上由某些有理函数$r_n(x)$导出的置换，这些函数可用来构造新的RSA系统。

设$a\neq 0$是一非平方整数，

$$\left(\frac{a}{p}\right)=-1,\quad \left(\frac{a}{q}\right)=-1$$

这里p，q是不同的奇素数。令

$$(x+\sqrt{a})^n=g_n(x)+h_n(x)\sqrt{a}$$

其中$g_n(x)$，$h_n(x)$是z上多项式，$g_n(x)$，$h_n(x)$可表示如下：

$$g_n(x)=\sum_{i=0}^{\left[\frac{n}{2}\right]}\binom{n}{2i}a^i x^{n-2i}$$

$$h_n(x)=\sum_{i=0}^{\left[\frac{n}{2}\right]}\binom{n}{2i+1}a^i x^{n-2i-1}$$

里德定义有理函数

$$f_n(x)=\frac{g_n(x)}{h_n(x)}$$

并证明如果素数$p\neq 2$，$2\nmid n$，$(n,p+1)=1$，$p\nmid n$，则$f_n(x)$是模p的置换有理函数。

易见，$f_n(x)$满足

$$\left(\frac{x+\sqrt{a}}{x-\sqrt{a}}\right)^n=\frac{f_n(x)+\sqrt{a}}{f_n(x)-\sqrt{a}}$$

由此可得

$$\frac{f_{kn}(x)+\sqrt{a}}{f_{kn}(x)-\sqrt{a}}=\frac{f_k(f_n(x))+\sqrt{a}}{f_k(f_n(x))-\sqrt{a}}$$

因此有

$$f_k(f_n(x)) = f_{kn}(x) = f_n(f_k(x))$$

这是构造RSA系统所需的一个最基本性质。

可以证明映射

$$\pi_k: Z/(p) \to Z/(p), \quad \pi_k(b) = f_k(b)$$

满足$\pi_k = \pi_n$当且仅当$k \equiv n(\mathrm{mod}(p+1))$。注意$f_1(x) = x$，$\pi_1 = \varepsilon$（单位映射）。这样，不难证明在$z/(p)$上有

引理2·1 在$Z/(p)$上有$f_k(f_n(x)) = f_n(f_k(x)) = f_1(x) = x$当且仅当

$$kn \equiv 1(\mathrm{mod}(p+1)) \qquad (2.5)$$

综合上述结果，可以看出，$f_n(x)$可用来构造新的RSA系统。

设$m = pq$，p，q是不同的大素数，p，q是保密的。设n是正的奇整数，满足

$$p \nmid n, \quad q \nmid n, \quad (n, p+1) = (n, q+1) = 1$$

取a是一非平方整数满足

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$$

则$f_n(x)$是模m的一个置换有理函数。构造加密密钥

$$E_R = f_n(x)(\mathrm{mod}\ m) \qquad (2.6)$$

解密密钥

$$D_R = f_k(x)(\mathrm{mod}\ m) \qquad (2.7)$$

其中k满足

$$nk \equiv 1 \pmod{[p+1,\ q+1]}$$

这样就构造出了一个密码系统。同样，在不知道m的因子p，q的情况下，从加密密钥（2.6）几乎不可能求出解密密钥（2.7）。因此上面构造的密码系统是一种RSA系统。

1965年，诺鲍尔证明，除开a的无平方因子部分是3且$3|n$外，存在无限多个素数p，q满足

$$(p+1,\ n)=(q+1,\ n)=1$$

$$\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=-1$$

其中n是奇数，a是非平方数。这个结果表明用置换有理函数构造RSA系统也是很有意义的。

4. 置换多项式与一致分布

本节介绍置换多项式对剩余类环上序列的一致分布的应用。

设m是一正整数，$\{a_n\}$是一整数序列。定义$\{a_n\}$关于模m的分布函数为

$$F_m(k)=\lim_{x\to\infty}\frac{1}{x}\left|\{a_n \mid n\leqslant x,\ a_n\equiv k \pmod{m}\}\right|$$

也就是说，$F_m(k)$是序列$\{a_n\}$中满足$n\leqslant x$，$a_n\equiv k \pmod{m}$的a_n的个数。如果$F_m(k)$是一有限的常

数，即

$$F_m(1)=F_m(2)=\cdots=F_m(m)$$

从

$$\sum_{i=1}^{m}F_m(i)=\lim_{x\to\infty}\frac{1}{x}|\{a_n|n\leqslant x\}|=1$$

得

$$F_m(1)=F_m(2)=\cdots=F_m(m)=\frac{1}{m}$$

此时称序列模m是一致分布的。一致分布是数论的一个重要课题。

如果序列$\{a_n\}$满足

(i) $\{a_n|(a_n,m)=1\}$是无限集。

(ii)对$1\leqslant j\leqslant m$，$(j,m)=1$，恒有

$$F_m^*(j)=\lim_{x\to\infty}\frac{|\{a_n|n\leqslant x,a_n\equiv j(\mathrm{mod}\,m)\}|}{|\{a_n|n\leqslant x,(a_n,m)=1\}|}$$

$$=\frac{1}{\varphi(m)}$$

则称序列$\{a_n\}$模m是弱一致分布的。

在数论里，主要考虑算术函数$\{f(n)\}$作成的序列的一致分布。在这里，我们考虑当$f(x)$是一整系数多项式时，序列$\{f(n)\}$的一致分布情况。

定理2·2 设$f(x)\in Z[x]$，$m=\prod_{i=1}^{k}p_i^{q_i}$是$m$的标准分解式。

(i)序列$\{f(n)|n=1,2,\cdots\}$是模m的一致分布序列当且仅当多项式$f(x)$是模m的置换多项式。

(ii)序列$\{f(n)|n=1,2\cdots\}$是模m的弱一致分布序列当且仅当多项式$f(x)$是模$p_i(i=1,\cdots,k)$的正则置换多项式。

证 (i)因为$f(x)$是一整系数多项式，故有$f(n)\equiv f(n+m)(\bmod\ m)$对任何正整数$n$成立。于是$\{f(n)\}$是一个周期序列(在模$m$的意义下)，且$m$是一个周期。利用这个事实得出，对$1\leqslant k\leqslant m$有

$$\begin{aligned}F_m(k) &= \lim_{x\to\infty}\frac{1}{x}|\{f(n)|1\leqslant n\leqslant x,\ f(n)\\ &\qquad \equiv k(\bmod\ m)\}|\\ &= \lim_{x\to\infty}\frac{1}{x}|\{f(n)|\ 1\leqslant n\leqslant m\left[\frac{x}{m}\right],\\ &\qquad f(n)\equiv k(\bmod\ m)\}|\\ &+ \lim_{x\to\infty}\frac{1}{x}|\{f(n)|\ m\left[\frac{x}{m}\right]\leqslant n\leqslant x,\\ &\qquad f(n)\equiv k(\bmod\ m)\}|\\ &= \lim_{x\to\infty}\frac{1}{x}\left[\frac{x}{m}\right]|\{f(n)|\ 1\leqslant n\leqslant m,\\ &\qquad f(n)\equiv k(\bmod\ m)\}|\\ &= \frac{1}{m}|\{f(n)|1\leqslant n\leqslant m,\end{aligned}$$

$$f(n)\equiv k \pmod{m}\}|$$

于是$\{f(n)\}$是模m的一致分布序列当且仅当对所有$1\leqslant k\leqslant m$有

$$|\{f(n)\,|\,1\leqslant n\leqslant m, f(n)\equiv k \pmod{m}\}|=1$$

即$f(x)$是模m的置换多项式。(i)得证。

对于(ii)，我们仅指出其证明思路，详细证明可参看纳克维兹[33]。首先证明若$(m_1, m_2)=1$，则$\{f(n)\}$是模m的弱一致分布当且仅当$\{f(n)\}$是模m_1和模m_2的弱一致分布。然后用类似于定理1·5的证明方法证明$\{f(n)\}$是模p^k的弱一致分布当且仅当$f(x)$是模p的正则置换多项式。

定理2·2说明多项式模m的一致分布和弱一致分布已完全化为模p的置换多项式及正则置换多项式。因此，剩余类环上的置换多项式亦可当作一致分布论的一个分支。

对给定的算术函数$\{f(n)\}$，定义两个量$M(f)$和$M^*(f)$如下：

$$M(f)=\{m\,|\,\{f(n)\}\text{是模}m\text{的一致分布}\}$$

$$M^*(f)=\{m\,|\,\{f(n)\}\text{是模}m\text{的弱一致分布}\}$$

当f是多项式时，易见$M(f)$就是第一章中介绍的置换谱，而

$$M^*(f)=\{p_1^{a_1}\cdots p_s^{a_s}\,|\,p_i\in s(f),\ a_i\geqslant 1\}$$

在一致分布论中，决定$M(f)$和$M^*(f)$是一重要的问题。泽门有下述重要结果：

定理2·3 设M是由正整数组成的一个集，则存在一个函数f使$M(f)=M$当且仅当M具有下述性质：

"如果$n\in M$，$d|n$，则$d\in M$"

定理2·3刻画出了形如$M(f)$这种数集的性质。对应于$M^*(f)$，是否有类似的结果呢？这是一个没有解决的问题。与此相关有下述

猜想 设M^*是由正整数组成的一个集，则存在一个函数f使$M^*(f)=M^*$当且仅当M^*具有下述性质：

"如果$n\in M^*$，$d|n$，d被n的所有素因子整除，则$d\in M^*$"。

当$d|m$，d被m的所有素因子整除时，有公式$\frac{m}{d}\varphi(d)=\varphi(m)$。于是对$1\leqslant j\leqslant d$，$(j,d)=1$有

$(j,m)=1$且（令$f(k)=a_k$）

$$F_d^*(j)=\lim_{x\to\infty}\frac{|\{a_k|k\leqslant x,\ a_k\equiv j(\mathrm{mod}\ d)\}|}{|\{a_k|k\leqslant x,\ (a_k,d)=1\}|}$$

$$=\lim_{x\to\infty}\frac{\sum_{i=0}^{\frac{m}{d}-1}|\{a_k|k\leqslant x,a_k\equiv j+di(\mathrm{mod}\ m)\}|}{|\{a_k|k\leqslant x,\ (a_k,m)=1\}|}$$

$$=\sum_{i=0}^{\frac{m}{d}-1}\lim_{x\to\infty}\frac{|\{a_k\,|\,k\leqslant x,\ a_k\equiv j+di(\bmod m)\}|}{|\{a_k\,|\,k\leqslant x,\ (a_k,m)=1\}|}$$

$$=\sum_{i=0}^{\frac{m}{d}-1}F_m^*\ (j+di)\qquad(2.8)$$

如果$\{a_k\}$是模m的弱一致分布序列，则有

$$F^*{}_m(j+di)\ =\frac{1}{\varphi(m)}$$

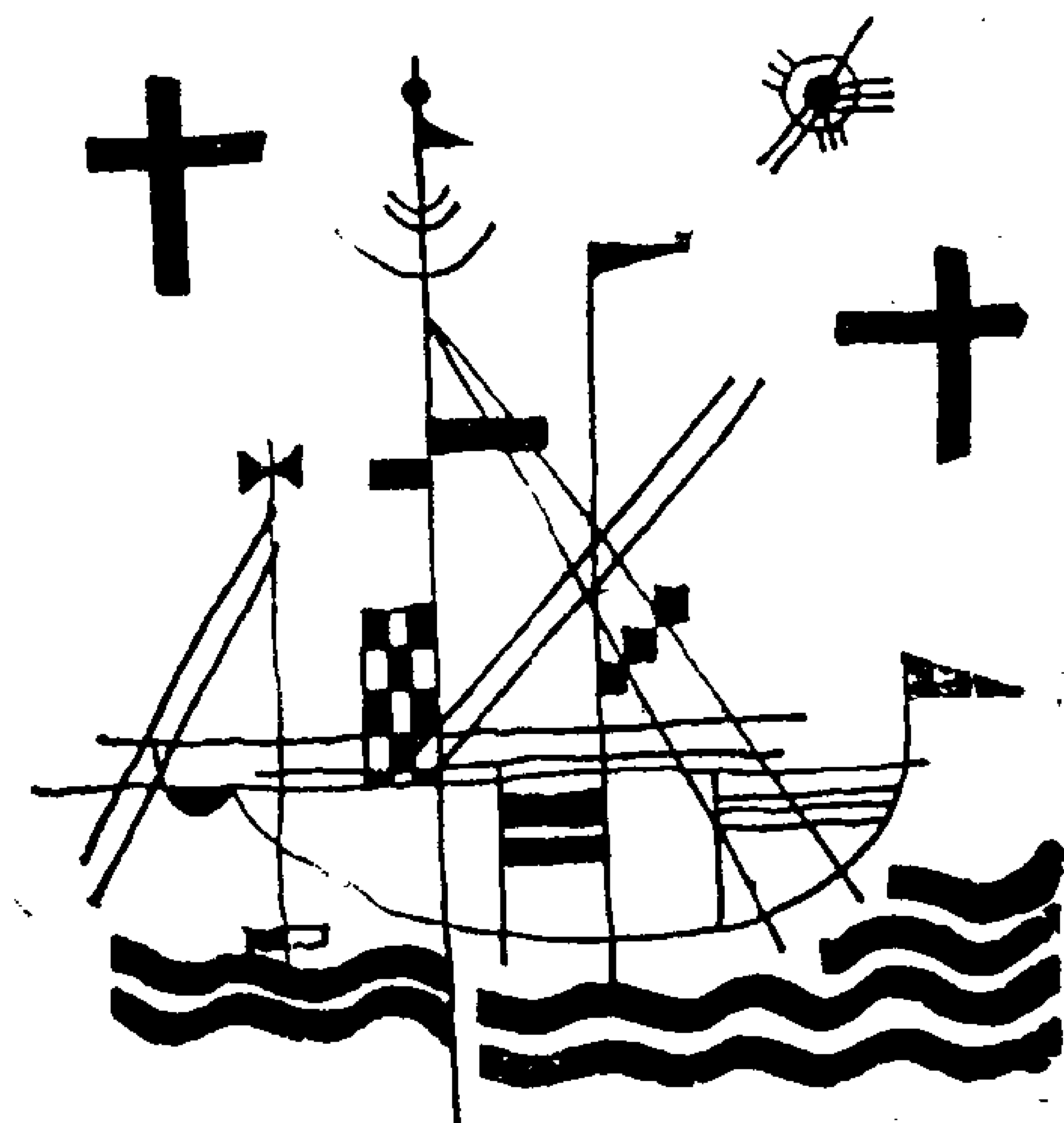
再由（2.8）得

$$F^*{}_d(j)=\frac{m}{d}\cdot\frac{1}{\varphi(m)}=\frac{1}{\varphi(d)}$$

因此$\{a_k\}$也是模d的弱一致分布序列．这就证明了上述猜想的必要性成立。

对充分性，猜想是一个困难的问题。到目前为止，最好的结果是由罗索丘维兹女士证明的。她证明，当M^*不含偶数时，上述猜想成立。

三　有限域上的置换多项式



在第一章里，我们已看出剩余类环$Z/(m)$的置换多项式被归结为有限素域F_p的置换多项式。作为一个推广，本章讨论任意有限域F_q的置换多项式。前两节介绍置换多项式的判别与构造。第三节考虑置换多项式在合成运算下生成的群。第四节应用有限域上方程的理论来研究置换多项式。最后，第五节介绍置换多项式的一个新兴方面——完全映射。

1. 置换多项式的判别

在本章里，我们总设F_q是q个元的有限域，其中$q=p^k$，p是一个素数。

设$f(x)\in F_q[x]$。如果f：$c\longmapsto f(c)$是F_q到F_q的一一映射（即导出F_q的一个置换），则称$f(x)$是F_q的置换多项式。

因为F_q仅有有限个元，类似于引理1·6不难看出置换多项式可以有下述几个等价的定义。

引理3·1 设$f\in F_q[x]$。则f是F_q的置换

多项式当且仅当以下条件之一成立。

(i) 函数f：$c \longmapsto f(c)$是单射，

(ii) 函数f：$c \longmapsto f(c)$是满射，

(iii) 对任何$a \in F_q$，$f(x) = a$在F_q中有解，

(iv) 对任何$a \in F_q$，$f(x) = a$在F_q中有唯一解。

类似于第一章，有限域F_q到自身的任一函数均可由某一次数小于q的多项式表出。事实上，设$\phi(x)$是F_q到F_q的任一函数，令

$$g(x) = \sum_{c \in F_q} \phi(c)\left(1 - (x-c)^{q-1}\right) \quad (3.1)$$

容易验证，$g(c) = \phi(c)$ 对所有$c \in F_q$成立，且$\deg(g(x)) < q$。因此，研究表F_q的全部元的函数归结为研究F_q的置换多项式。这是很多其它环所不具有的性质。

由$F_q[x]$中的欧几里得辗转相除法得

引理3·2 设f，$g \in F_q[x]$。则$f(c) = g(c)$对所有$c \in F_q$均成立当且仅当$f(x) \equiv g(x) \pmod{x^q - x}$

利用这个引理及欧几里得算法得到，$F_q[x]$中任一多项式$f(x)$模$(x^q - x)$后均可化为一个次数小于q的$F_q[x]$中的多项式$g(x)$，且这种$g(x)$是唯一确定的。这个确定的$g(x)$称为$f(x)$的简化多项式，而$\deg(g(x))$称为$f(x)$的简化次数。

现在我们来证明厄米特在1863年证明的判别法则。

定理3·3 设F_q的特征为p，$f(x)\in F_q[x]$。则f是F_q的置换多项式当且仅当下面两个条件成立：

(i) f在F_q中恰有一个零点。

(ii) 对每一整数t，$1\leqslant t\leqslant q-2$，都有$f^t(x)$模$(x^q-x)$的简化次数不超过$q-2$。

证 设$N(a)$表示$f(x)=a$在F_q中的解数。则f是F_q的置换多项式$\Longleftrightarrow N(a)=1$对所有$a\in F_q$成立$\Longleftrightarrow N(a)\equiv 1\pmod p$对所有$a\in F_q$均成立。（由$N(a)\equiv 1\pmod p$推出$N(a)>0$，故$N(a)=1$，对所有的$a\in F_q$）

假设

$$f^t(x)\equiv\sum_{i=0}^{q-1}b_i^{(t)}x^i\ (\mathrm{mod}\,(x^q-x)),$$

$$0\leqslant t\leqslant q-1.$$

则因

$$\sum_{x\in F_q}x^i=\begin{cases}0, & 0\leqslant i\leqslant q-2\\ -1, & i=q-1\end{cases}$$

得

$$\sum_{c\in F_q}f^t(c)=\sum_{i=0}^{q-1}b_i^{(t)}\sum_{c\in F_q}c^i$$

$$=b_{q-1}^{(t)}\sum_{c\in F_q}c^{q-1}$$

$$=-b_{q-1}^{(t)}\qquad(0\leqslant t\leqslant q-1)$$

我们考虑$N(a)$的值如下.

$$N(a)\equiv\sum_{c\in F_q}(1-(f(c)-a)^{q-1})\pmod p$$

$$\equiv-\sum_{c\in F_q}(f(c)-a)^{q-1}\pmod p$$

$$\equiv-\sum_{c\in F_q}\sum_{t=0}^{q-1}\binom{q-1}{t}f(c)^t$$

$$(-a)^{q-1-t}\pmod p$$

$$\equiv\sum_{t=0}^{q-1}\binom{q-1}{t}b_{q-1}^{(t)}(-a)^{q-1-t}$$

$$\pmod p$$

$$\equiv b_{q-1}^{(q-1)}+\sum_{t=0}^{q-2}\binom{q-1}{t}b_{q-1}^{(t)}$$

$$(-a)^{q-1-t}\pmod p\qquad(3.2)$$

如果条件（i）成立，则$\sum_{c\in F_q}f(c)^{q-1}=-1$，

即有$b_{q-1}^{(q-1)}=1$．如果还有（ii）成立，则$b_{q-1}^{(t)}=0\ (0\leqslant t\leqslant q-2)$．将这些结果代入（3·2）得$N(a)\equiv1\pmod p$对所有$a\in F_q$均成立．因此，$f(x)$是$F_q$的置换多项式．

反之，因$f(x)$是置换多项式，（i）当然成

立。又$N(a)\equiv 1 \pmod p$恒成立，故由（3.2）得

$$\sum_{t=0}^{q-2}\binom{q-1}{t}b_{q-1}^{(t)}(-a)^{q-1-t}$$
$$+b_{q-1}^{(q-1)}-1=0 \qquad (3.3)$$

对所有$a\in F_q$均成立。（3.3）左端是一个次数小于$(q-1)$的，以a为变元的多项式，该多项式必须恒为零，即有

$$b_{q-1}=1,\ \binom{q-1}{t}b_{q-1}^{(t)}=0$$
$$(0\leqslant t\leqslant q-2)$$

根据卢卡斯引理，$\binom{q-1}{t}\not\equiv 0 \pmod p$对$0\leqslant t\leqslant q-1$均成立，故得

$$b_{q-1}^{(t)}=0 \quad (0\leqslant t\leqslant q-2)$$

这就证明了条件（ii）成立。

定理至此全部证完。

推论3·4 设$d>1, d\mid q-1$。则不存在次数为d的F_q的置换多项式。

证 设$f(x)$的次数为$d, d>1, d\mid q-1$，只需取$t=\frac{q-1}{d}$，故$f^t(x)$的简化次数为$q-1$，由定理3·3便知。

定理3·3还可改述为

定理3·5 设F_q的特征为p，$f\in F_q[x]$。则f是F_q的置换多项式当且仅当下面两个条件成

立：

(i) $f_{(x)}^{q-1}$ 的简化次数是 $(q-1)$。

(ii) $f_{(x)}^{t}(1\leqslant t\leqslant q-2)$ 的简化次数不超过 $q-2$。

证　若 $f(x)$ 是 F_q 的置换多项式。则在定理3·3的最后一部分证明中已得出 $b_{q-1}^{(q-1)}=1\neq 0$，$b_{q-1}^{(t)}(1\leqslant t\leqslant q-2)=0$。这就表明条件(i)，(ii)成立。

反过来，若 $b_{q-1}^{(q-1)}\neq 0$，$b_{q-1}^{(t)}=0$ $(1\leqslant t\leqslant q-2)$。因 $b_{q-1}^{(0)}$ 总是零。代入（3.2）得出

$$N(a)\equiv b_{q-1}^{(q-1)}\neq 0 \pmod p$$

对所有 $a\in F_q$ 均成立。即 $f(x)=a$ 在 F_q 中总有解，由引理3·1立得定理。

类似于定理1·4，可以证明

定理3·6　设特征 p 为奇数。若 f，g 均是 F_q 的置换多项式，则 fg 不是 F_q 的置换多项式。

当特征 $p=2$ 时，定理3·6不成立。例如取 $f=g=x^2$，则 f，g，fg 均为 F_{2^k} 的置换多项式。于是，自然地提出下述

问题　若 f，g 是 F_{2^k} 的置换多项式。在什么条件下 fg 也是 F_{2^k} 的置换多项式？

孙琦、旷京华[44]曾经证明：设 K 是一个 n 次代数数域，A 是 K 上的一个理想，$N(A)$ 代表模 A 剩余类的个数，$A\neq P_1\cdots P_f$，$P_i|$〔2〕，这里 P_i 是不

同素理想，$(j=1,\cdots,f)$，如果$\alpha_1,\cdots,\alpha_{N(A)}$和$\beta_1,\cdots,\beta_{N(A)}$分别是$A$的二个完全剩余系，则$\alpha_1\beta_1,\cdots,\alpha_{N(A)}\beta_{N(A)}$不是$A$的完全剩余系。

2. 置换多项式的构造

由于在判别任意一个多项式是否是置换多项式时，没有有效的一般方法，因此，考虑特殊形状的置换多项式就显得更有意义。本节的目的就在于介绍这方面的结果。

最简单的情形是

定理3·6 (i)F_q上每一个线性多项式$ax+b$ $(a\neq 0)$是F_q的置换多项式。

(ii)单项式x^n是F_q的置换多项式当且仅当$(n, q-1)=1$。

证 (i)显然成立。(ii)由有限域的结构立得。

定理3·7 设F_q的特征为p，则p—多项式

$$L(x)=\sum_{i=0}^{m}a_i x^{p^i}\in F_q[x]$$

是F_q的置换多项式当且仅当$L(x)$在F_q中只有唯一解$x=0$。

证 因$(x+y)^p=x^p+y^p$在有限域中成立，故$L(x)=L(y)$当且仅当$L(x-y)=0$。由此看

出，$L(x)$是F_q的置换多项式当且仅当 $L(x)$ 在F_q中仅有一根，即$x=0$（$x=0$显然是$L(x)$的一个根）。

完全类似于定理1·10有

定理3·8 设 r 是正整数，$(r, q-1)=1$，s 是$(q-1)$的正因子。再设$g(x)\in F_q[x]$使得$g(x^s)$在F_q中无非零根。则 $f(x)=x^r g(x^s)^{\frac{q-1}{s}}$ 是F_q的置换多项式。

定理1·12可推广到有限域的情形，即

定理3·9 设$a\in F_q^*$。则迪克逊多项式

$$g_k(x,a)=\sum_{j=0}^{[\frac{k}{2}]}\frac{k}{k-j}\binom{k-j}{j}(-a)^j x^{k-2j}$$

是F_q的置换多项式当且仅当$(k, q^2-1)=1$；进一步，$g_k(x,a)$是F_q的正则置换多项式当且仅当有$(k, p(q^2-1))=1$。

设$f\in F_q[x]$，b，c，$d\in F_q$，$c\neq 0$。易见 f 是F_q的置换多项式当且仅当 $f_1(x)=cf(x+b)+d$ 是F_q的置换多项式。适当选取b，c，d 可使 f_1 成为标准形，即满足$f_1(0)=0$，f_1是首1的，且当特征 p 不整除 f 的次数 n 时，f_1的x^{n-1}的系数为 0。这样，只需研究标准形状的置换多项式。利用厄米特准则，迪克逊决定了所有次数不超过 5 的标准形置换多项式，见下表。迪克逊也决定了当 q

为奇数时，F_q的所有次数为 6 的标准形置换多项式。当次数大于 6 时，只有一些零碎的结果，没有比较完全的标准形置换多项式表。

次数不超过 5 的标准形置换多项式表

F_q的标准形置换多项式	q 值
x	任何 q
x^2	$q\equiv 0(\mathrm{mod}\ 2)$
x^3	$q\not\equiv 1(\mathrm{mod}\ 3)$
x^3-ax（a 非平方）	$q\equiv 0(\mathrm{mod}\ 3)$
$x^4\pm 3x$	$q=7$
$x^4+a_1x^2+a_2x$（且$x=0$是其唯一根）	$q\equiv 0(\mathrm{mod}\ 2)$
x^5	$q\not\equiv 1(\mathrm{mod}\ 5)$
x^5-ax（a 非四次方）	$q\equiv 0(\mathrm{mod}\ 5)$
$x^5+ax(a^2=2)$	$q=9$
$x^5\pm 2x$	$q=7$
$x^5+ax^3\pm x^2+3a^2x$（a非平方）	$q=7$
$x^5+ax^3+5^{-1}a^2x$	$q\equiv\pm 2(\mathrm{mod}\ 5)$
$x^5+ax^3+3a^2x$（a 非平方）	$q=13$
$x^5-2ax^3+a^2x$（a 非平方）	$q\equiv 0(\mathrm{mod}\ 5)$

下面讨论由二项式构成的置换多项式问题。

定理3·10 设$q\equiv 1(\mathrm{mod}\ 2)$，$f(x)=x^{\frac{q-1}{2}+m}+ax^m\in F_q[x]$，$m$是正整数。则有

(i) 当$(m,q-1)=1$时，$f(x)$是F_q的置换多

项式当且仅当存在$c\in F_q^*$，$c^2\neq 1$使

$$a=\frac{(1+c^2)}{(1-c^2)}$$

(ii)当$(m,q-1)=2$时，$f(x)$是F_q的置换多项式当且仅当$q\equiv 3(\mathrm{mod}\ 4)$，且存在$F_q$中的非平方元$c$使

$$a=\frac{1+c}{1-c}$$

(iii)当$(m,q-1)=d\geqslant 3$时，$f(x)$不是F_q的置换多项式。

证 考虑方程

$$x_1^m\left(x_1^{\frac{q-1}{2}}+a\right)=x_2^m\left(x_2^{\frac{q-1}{2}}+a\right),$$

$$x_1,x_2\in F_q. \tag{3.4}$$

显然，$f(x)$是F_q的置换多项式当且仅当(3.4)无$x_1\neq x_2$的解。现设$x_1\neq x_2$满足(3.4)，我们来推出a应满足的条件。

(i)$(m,q-1)=1$。当x_1x_2是F_q的平方元时(包括$x_1=0$或$x_2=0$的情形)，(3.4)有解$x_1\neq x_2$当且仅当$a=\pm 1$。当x_1x_2是F_q中的非平方元时，不失一般，可设x_1为平方元，x_2为非平方元。此时有$x_1^{\frac{q-1}{2}}=1$，$x_2^{\frac{q-1}{2}}=-1$，且(3.4)成立$\Longleftrightarrow$

$$a=\frac{x_2^m+x_1^m}{x_2^m-x_1^m}=$$

$$\left(1+\left(\frac{x_1}{x_2}\right)^m\right)\Big/ 1-\left(\frac{x_1}{x_2}\right)^m$$

$\Longleftrightarrow$存在F_q中的非平方元 t （令 $t=\left(\frac{x_1}{x_2}\right)^m$），使得

$$a=\frac{1+t}{1-t}$$

因此，（3.4）无解$x_1\neq x_2$的充要条件是$a\neq\pm1$，且对任何非平方元$t\in F_q$有 $a\neq(1+t)(1-t)^{-1}$。这两个条件等价于存在$c\in F_q^*$，$c^2\neq1$使

$$a=\frac{1+c^2}{1-c^2}$$

(ii) $(m,q-1)=2$。当$q\equiv1(\bmod\ 4)$时，$x_2=-x_1$是（3.4）的满足$x_1\neq x_2$的解，$f(x)$不是F_q的置换多项式。当$q\equiv3(\bmod\ 4)$时，此时可仿(i)证明(ii)成立。

(iii) $(m,q-1)=d\geqslant3$。设ω是F_q的一个 d 次本原根，则$x_1=1$，$x_2=\omega^2$是（3.4）的满足$x_1\neq x_2$的解。因此，$f(x)$不是F_q的置换多项式。□

用类似的方法还可以证明

定理3·11 设 $m>1$，$m|q-1$。则二项式 $x^{\frac{q-1}{m}+1}+ax(a\neq0)$是$F_q$的置换多项式当且仅当

(i) $(-a)^m\neq1$。

(ii) 设 c 是F_q的一个固定的m次本原根，则对所有$0\leqslant i<j\leqslant m-1$有

$$\left(\frac{a+c^i}{a+c^j}\right)^{\frac{q-1}{m}}\neq c^{j-i}.$$

上面两个定理说明，存在形如 $x^{\frac{q-1}{2}+1}+ax$ $(a\neq 0)$的F_q的置换多项式。1962年[10]，卡里兹证明这样的多项式不是F_q的任何扩域 $F_{q^r}(r>1)$的置换多项式。这是很有意思的结果，它将建议一些置换多项式的重要性质。卡里兹的结果可叙述为

定理3·12 设$q\equiv 1(\mathrm{mod}\ 2)$，$a\neq 0$.则$f(x)=x^{\frac{q-1}{2}+1}+ax$不是$F_{q^r}(r>1)$的置换多项式。

证 如果 $2|r$，则$\left.\frac{q+1}{2}\right|q^r-1$，利用推论3.4即得。下设 $2\nmid r$.取$m=\frac{q-1}{2}$，则$q^r\equiv -1\equiv m(\mathrm{mod}(m+1))$，于是有正整数 k 使 $q^r=k(m+1)+m$.从$k(m+1)\equiv m+1(\mathrm{mod}\ q)$及$(m+1,q)=1$知$k\equiv 1(\mathrm{mod}\ q)$。根据厄米特准则，只需证明

$$(x^{m+1}+ax)^{k+m-1}\quad(\mathrm{mod}(x^{q^r}-x))$$

的简化次数为q^r-1。现在

$$(x^{m+1}+ax)^{k+m-1}=\sum_{j=0}^{k+m-1}\binom{k+m-1}{j}$$

$$a^j x^{(m+1)(k+m-1-j)+j}$$

$$=\sum_{j=0}^{k+m-1}\binom{k+m-1}{j}a^j x^{q^r-1+m^2-m-jm}$$

$$=\binom{k+m-1}{m-1}a^{m-1}x^{q^r-1}+H(x)$$

其中$H(x)$是上面和式中除去$j=m-1$这一项所剩下的和。当$j\geqslant m$时，$q^r-1+m^2-m-jm\leqslant q^r-2$；当$j\leqslant m-2$时，因$r>1$，故$q^r\leqslant q^r-1+m^2-m-jm\leqslant 2q^r-3$。因此，$H(x)$模$(x^{q^r}-x)$的简化次数不超过$q^r-2$。剩下只需证明特征$p$不整除二项式系数

$$\binom{k-1+m}{m-1}$$

因$k-1\equiv 0 \pmod q$，$m<q$，$m\not\equiv 0 \pmod p$，故由卢卡斯引理得

$$\binom{k-1+m}{m-1}\equiv\binom{m}{m-1}=\binom{m}{1}$$

$$=m\not\equiv 0 \pmod p$$

结论成立。□

1962年，卡里兹猜想定理3·12的结论对形如$x^{\frac{q+1}{3}}+ax$的二项式也成立。利德尔和詹姆斯前不久证明，当特征$p>5$时卡里兹的这个猜想成立。最近[7]，我们用较复杂的方法完全证实了卡里兹的这个猜想。于是有

定理3·13 设$q\equiv 1 \pmod 3$，$a\in F_q^*$，则二

项式 $x^{\frac{q-1}{3}+1}+ax$不是F_{p^r} $(r>1)$的置换多项式。

上述两个定理建议下述更一般的问题。

问题 设$m>1$是正整数,$q\equiv1(\mathrm{mod}\ m)$, $a\in F_q^*$. 能否证明 $x^{\frac{q-1}{m}+1}+ax$不是F_{q^r} $(r>1)$的置换多项式。

当特征 p 比较大时,这个问题比较容易解决。困难的是小特征 p 的情形。

定理3·12和定理3·13还建议，若$f\in F_q[x]$, f 是F_q的所有扩域F_{q^r}的置换多项式，则这种多项式 f 是相当稀少的。事实上，这种多项式可以被完全决定如下。

定理3·14 设$f\in F_q[x]$。则 f 是F_q 的所有扩域的置换多项式当且仅当 $f(x)=ax^{p^h}+b$，其中 h 是某个非负整数，$a\neq0$， p 是F_q的特征。

证 因$(p^h,q^r-1)=1$，充分性是显然的。现证必要性。

因 f 是F_q的置换多项式，对F_q中每一元 c，方程$f(x)=c$在F_q中有唯一解 d 。于是

$$f(x)-c=(x-d)^kg(x)$$

其中 k 是正整数，$g(x)\in F_q[x]$，$\deg(g(x))=0$ 或 g 是$F_q[x]$中次数大于1的不可约因子g_i之积。如果有一g_i，$\deg(g_i)\geqslant2$，取 r 是 $\deg(g_i)$ 的正倍数，则g_i在F_{q^r} 中有一根。这样，f 就不是F_{q^r}

的置换多项式。因此，必有

$$f(x)-c=a(x-d)^k,\quad a\neq 0 \qquad (3.5)$$

分别取$c=0$和$c=-1$，知存在d_0，$d_1\in F_q$使

$$a(x-d_0)^k-a(x-d_1)^k=1$$

作变换$x\longrightarrow x+d_1$得

$$a(x+d_1-d_0)^k-ax^k=1$$

$$=a\sum_{j=0}^{k-1}\binom{k}{j}x^j(d_1-d_0)^{k-j}$$

因$d_0\neq d_1$，比较系数得

$$\binom{k}{j}\equiv 0\pmod p\ (0<j<k) \qquad (3.6)$$

设$p^h\leqslant k<p^{h+1}$，h是非负整数。如果$k\neq p^h$，取$j=p^h$，由卢卡斯引理得

$$\binom{k}{p^h}\not\equiv 0 \pmod p$$

与（3.6）矛盾。因此必有$k=p^h$。再由（3.5）即得定理。□

用有限域上的类似黎曼假设，可以证明

定理3·15 设$k>2$，k不是特征p的方幂。如果$q\geqslant(k^2-4k+6)^2$，则$x^k+ax(a\neq 0)$不是F_q的置换多项式。

对更一般的二项式，即$f(x)=x^k+ax^j$的情形，也有类似结果。

3. 置换多项式的群

设$f(x)$，$g(x)$是F_q上次数小于q的置换多项式，则多项式f和g的合成$f(g(x))$模(x^q-x)后仍为F_q上次数小于q的置换多项式。因此，在合成运算下，F_q的所有次数小于q的置换多项式作成一群。该群同构于q个字母上的对称群S_q。事实上，对F_q的任一次数小于q的置换多项式$f(x)$，$f(x)$导出F_q的一个置换σ_f。作映射

$$\varphi:\ f\longmapsto\sigma_f$$

则φ是从F_q的所有次数小于q的置换多项式到F_q的全体置换的映射。不同的$f(x)$导出不同的置换σ_f，因此φ是单射。对F_q的任一置换σ，由拉格朗日插值公式知，存在F_q上一次数小于q的多项式$f(x)$使$f(c)=\sigma(c)$对所有$c\in F_q$均成立，于是f导出σ，故φ是满射。进一步，直接验证知φ满足

$$\varphi(f(g))=\sigma_{fg}=\sigma_f\cdot\sigma_g=\varphi(f)\cdot\varphi(g)$$

因此φ是一个同构映射。

上面的讨论指出，对称群S_q及其子群可用F_q的置换多项式群来表示。从这个观点出发，可以预料置换多项式在群论中是很有用的。

定理3·16 设$q>2$，则S_q由x^{q-2}及F_q上所

有线性多项式生成。

证 首先，x^{q-2}及所有F_q的线性多项式均是F_q的置换多项式，因此都是S_q中的元。其次，从对换$(bc)=(ob)(oc)(ob)$及S_q由所有对换生成这两个事实知，只需证明对换(oa)可被x^{q-2}及线性多项式$\alpha x+\beta(\alpha\neq 0)$的合成所表出。多项式

$$f_a(x) = -a^2[((x-a)^{q-2}+a^{-1})^{q-2} - a]^{q-2}$$

正好表出对换(oa)，即$f(0)=a$，$f(a)=0$，当$c\neq 0$，a时有$f_a(c)=c$。因为$f_a(x)$是由x^{q-2}及线性多项式合成而来，故定理的结论成立。□

从定理3·16不难看出有下述

定理3·17 设$q>2$，c是F_q的一个固定的本原根。则S_q由cx，$x+1$及x^{q-2}所生成。

类似地，可以得到交错群A_q的生成元，这里交错群A_q是由S_q的所有偶置换组成的。与偶置换相对应，如果F_q的置换多项式f导出F_q的一个偶置换，就称f是F_q的偶置换多项式。

引理3·18 设$q>2$，$a\in F_q$。则$x+a$和$(x^{q-2}+a)^{q-2}$是F_q的偶置换多项式；ax是偶置换多项式当且仅当a是F_q^*中的平方元；x^{q-2}是偶置换多项式当且仅当$q\equiv 3 \pmod 4$。

证 $x+a$导出的置换由p^{e-1}个形如$(\alpha, \alpha+a, \cdots, \alpha+(p-1)a)$的长度为$p$的圈组成，这

里$q=p^e$.因此，当$2\nmid p$或$q=2^e$而$e>1$时，$x+a$是偶置换多项式。

$(x^{q-2}+a)^{q-2}$由偶置换$x+a$及两个同样的置换x^{q-2}生成，因此$(x^{q-2}+a)^{q-2}$也是偶置换多项式。

ax是置换多项式当且仅当$a\neq 0$。设$a=c^s$，则ax由s个cx合成而来。cx导出的置换是一长度为$(q-1)$的圈，故当q为奇时，cx是奇置换。当q为偶数时，F_q中的每一个元都为平方元。由此推得，ax是F_q的偶置换多项式当且仅当$a\neq 0$，且a是F_q的平方元。

最后，x^{q-2}把$F_q-\{0,1,-1\}$的所有元素依对换双双配对。当$2\nmid q$时，共有$\frac{q-3}{2}$个对换；当$2|q$时，共有$\frac{q-2}{2}$个对换(此时$1=-1$)。故x^{q-2}是偶置换多项式当且仅当$q\equiv 3 \pmod 4$。□

设$q>2$，定义下列置换多项式的集。

$$L_q=\{ax+b \mid a\in F_q^*,\ b\in F_q\}$$

$$AL_q=\{(x^{q-2}+a)^{q-2} \mid a\in F_q\}$$

$$Q_q=\{a^2x+b \mid a\in F_q^*,\ b\in F_q\}$$

这些集在模(x^q-x)的合成运算下均作成群。容易证明

定理3·19 设$q>2$，c是F_q的一个本原根。

则

(i) L_q由cx和$x+1$生成，

(ii) Q_q由c^2x和$x+1$生成，

(iii) A_q由子群AL_q和Q_q生成，

(iv) A_q由$c^2x, x+1$和$(x^{q-2}+1)^{q-2}$生成。

类似于定理1·13，定义迪克逊多项式组成的多项式类如下：

$$P(0)=\{g_k(x,0) \mid k\text{是正整数}, (k,q^2-1)=1)\}$$

$$P(a)=\{g_k(x,a) \mid k\text{是正整数}, (k,q-1)=1\},\quad a\neq 0$$

则有

定理3·20 $P(a)$在合成运算下作成一群当且仅当$a=0, \pm 1$，进一步，当$a=0, \pm 1$时，还有$g_k(g_n(x,a), a)=g_{kn}(x,a)$。因此当$a=0$，$\pm 1$时，$P(a)$是阿贝尔群。

另一类与置换多项式有关的群是伯蒂一马修群。它是由伯蒂在1852年，马修在1862年独立引进的。

设F_{q^r}是F_q的扩域，考虑q一多项式

$$L(x)=\sum_{s=0}^{r-1}\alpha_s x^{q^s}\in F_{q^r}[x] \qquad (3.7)$$

定理3·7表明$L(x)$是F_{q^r}的置换多项式当且仅当$L(x)$仅有一个根在F_{q^r}中，即根$x=0$，从这个结

论出发，利用线性代数的知识可以证明形如(3.7)的置换多项式在模$(x^{q^r}-x)$的合成运算下作成一个群，这个群称为伯蒂一马修群。可以证明

定理3·21 上述伯蒂一马修群同构于F_q上$r\times r$阶非奇异矩阵在矩阵乘法下作成的一般线性群$GL(r,F_q)$。

4. 例外多项式

设f是$F_q[x]$中次数大于零的多项式。f是F_q的置换多项式等价于，对任何不同元a_1，$a_2\in F_q$均有$f(a_1)\neq f(a_2)$，即

$$\frac{f(a_1)-f(a_2)}{a_1-a_2}\neq 0$$

因此，$f(x)$是F_q的置换多项式当且仅当两个变元的多项式

$$\phi(x,y)=\frac{f(x)-f(y)}{x-y} \qquad (3.8)$$

在F_q中无$x\neq y$的解。如果$\phi(x,y)$在$F_q[x,y]$中有一不具有$a(x-y)$形状的绝对不可约因子，则当q充分大时，应用著名的兰一魏依定理知该因子在F_q中有一$x\neq y$的零点。这样，$\phi(x,y)$在F_q中就有$x\neq y$的零点，因此$f(x)$就不是F_q的置换多项

式。从这个观点出发，可以预料有限域上方程的深入理论可用到置换多项式的研究上，而置换多项式的判别有可能归结为绝对不可约多项式的研究。本节的目的就是介绍这方面的结果。

设$g(x,y)\in F_q(x,y)$。如果$g(x,y)$在F_q，的任何扩域上都是不可约的，则称 g 是F_q上的绝对不可约多项式。利用这个概念，假设

$$\phi(x,y)=a_n g_1\cdot g_2\cdot\cdots\cdot g_r \qquad (3.9)$$

是 ϕ 在$F_q[x,y]$中的标准分解式，其中a_n 是 f 的首项系数，$g_i[x,y]$是F_q中的首1不可约多项式。上面已经说明，若某一g_i在F_q上是绝对不可约的，且$g_i\neq a(x-y)$，则当 q 充分大时，f 不是F_q的置换多项式。这个结果导致下述

定义 在分解式（3.9）中，若F_q 上任一个绝对不可约的g_i均具有形状$a(x-y)$，则称 f 是F_q上的例外多项式。

利用例外多项式的概念，上述结果可叙述为

定理3·22 若 f 不是F_q上的例外多项式，则当 q 充分大时，f 不是F_q的置换多项式。

在素域F_p的情形，例外多项式的概念是由达文波特—刘易斯于1963年引进的。我们给出的定义与一般例外多项式的定义是不同的，利用上述新定义，关于置换多项式的结果可以得到更完备的阐述。

一个值得注意的问题是定理3·22的逆是否成立，即如果 f 是 $F_q[x]$ 中次数大于零的例外多项式，则当 q 充分大时，f 是不是 F_q 的置换多项式。

1967年[29]，麦克卢尔证明，若 f 是 F_q 上的例外多项式，特征 $p>\frac{1}{2}\deg(f)$，则 f 是 F_q 的置换多项式。1968年[43]，威廉斯给出了这一结果的一个简单证明。1970年[14]，科恩完全解决了定理3·22的逆问题，他用代数数论的方法证明了下述更强的结果。

定理3·23 设 f 是 $F_q[x]$ 中次数大于零的例外多项式，则 f 是 F_q 的置换多项式。

综合定理3·22和定理3·23得

定理3·24 设 f 是 $F_q[x]$ 中次数大于零的多项式。存在与 f 的次数 $\deg(f)=n$ 有关的常数 c_n，只要 $q>c_n$，则 f 是 F_q 的置换多项式当且仅当 f 是 F_q 的例外多项式。

如果 $q\leqslant c_n$ 时，定理3·24也成立，则定理3·24给出了判别置换多项式的一个理想准则。因此，决定定理3·24对 $q\leqslant c_n$ 是否成立是一有重要意义的问题。

下面我们介绍一个著名的猜想。

卡里兹猜想 给定一个正偶数 n，存在常数

c_n，只要奇$q>c_n$，则F_q无次数为n的置换多项式。

对卡里兹猜想，当$n=2^k$时比较容易解决(下面将证明这个事实)。迪克逊的置换多项式表解决了$n=2,4,6$的情形。1963年，达文波特和刘易斯解决了q为素数的情形（见定理1·19）。在q为素数的情形，朗比利和达文波特[8]，以及蒂特凡林[41]于1966年还得到了定量的结果。1967年[19]，海斯解决了$n=10$的情形。最近[6]，我们解决了$n=12$和14的情形。综合这些结果有

定理3·25 卡里兹猜想对$n<18$均成立。

根据定理3·24，卡里兹猜想可等价地叙述为：给定一个正偶数n，存在常数c_n，只要奇$q>c_n$，则F_q无次数为n的例外多项式。

定理3·26 给定一个正整数n，存在常数c_n，只要$q>c_n$，$(n,q)=1$，且F_q有一单位根$\xi\neq 1$，则F_q无n次置换多项式。

证 设$f\in F_q[x]$，$\deg(f)=n$。又设

$$\phi(x,y)=\frac{f(x)-f(y)}{x-y}=a_n g_1\cdots g_r \tag{3.10}$$

是ϕ在$\overline{F_q}[x,y]$中的标准分解式，此处$\overline{F_q}$为F_q的代数闭包，a_n是f的首项系数，g_i是$\overline{F_q}$上首1的绝对不可约多项式。若能证明，某一$g_i\in F_q[x,y]$，

且$g_i \neq a(x-y)$，则g_i是F_q上的绝对不可约多项式，且$g_i \neq a(x-y)$。由兰—魏依定理得定理成立。

设$h_i(1 \leqslant i \leqslant r)$是$g_i$的次数最高的齐次部分，显然有

$$\frac{x^n - y^n}{x - y} = h_1 \cdots h_r \qquad (3.11)$$

设ξ，…，ξ_{n-1}是$\overline{F_q}$的不等于1的所有n次单位根，（3.11）给出

$$(x - \xi_1 y) \cdots (x - \xi_{n-1} y) = h_1 \cdots h_r \qquad (3.12)$$

因$p \nmid n$, ξ_1，…，ξ_{n-1}是互不相同的，故$x - \xi y \in F_q[x,y]$恰整除h_i中的某一个，不妨设$(x - \xi y) \mid h_1$。

又设σ是$\overline{F_q}[x,y]$到自身的下述同构：

$$\sigma\left(\sum_{j,k} a_{jk} x^j y^k\right) = \sum_{j,k} a_{jk}^q x^j y^k \qquad (3.13)$$

将σ作用于（3.10）的两端。因$\phi \in F_q[x,y]$，故$\sigma(a_n) = a_n$，$\sigma(\phi) = \phi$，因此σ置换诸g_i。令$\sigma(g_1) = g_m$，此处$1 \leqslant m \leqslant r$，则$\sigma(h_1) = h_m$。$(x - \xi y)$在$\sigma$作用下保持不变，现有$(x - \xi y) \mid h_1$，故$x - \xi y$整除$\sigma(h_1) = h_m$。因$x - \xi y$恰整除$h_i$中的一个，即$h_1$，我们推得$h_m = h_1$，即$g_1 = \sigma(g_1)$，$g_1$在$\sigma$之下

不变。注意$\overline{F_q}$关于F_q的所有自同构由 σ 生成，这就意味着g_1在$\overline{F_q}$的任何自同构下不变。因此 $g_1 \in F_q[x,y]$，g_1是F_q上的绝对不可约多项式。从$(x-\xi y)|h_1$，$\xi\neq 1$知$g_1\neq a(x-y)$。因此 f 不是F_q上的例外多项式，由定理3·22即得。

推论3·27 设 n 是正偶数。存在c_n，只要$q>c_n$，$(n,q)=1$，则F_q上无 n 次置换多项式

证 在定理3·26中取$\xi=-1$立得。

特别，当$n=2^k$或 q 为素数时，卡里兹猜想成立。

推论3·28 设 n 为正整数，$(n,q)=1$，q 充分大，则F_q有次数为 n 的置换多项式当且仅当$(n,q-1)=1$。

证 若$(n,q-1)=1$，取$f(x)=x^n$即合所需。若$(n,q-1)>1$，则F_q有一单位根 $\xi\neq 1$，由定理3·26即得。

比卡里兹猜想更广泛一些，可以提出下述

猜想 设 n 是给定的正整数.存在常数c_n.只要$q>c_n$，且 n 不是特征 p 的方幂，则 F_q 无 n 次置换多项式。

当 n 为偶数时，上述猜想便化为卡里兹猜想。

以上的讨论表明有限域上方程的理论，主要是兰—魏依定理（这是类似黎曼假设的结果），

可用来证明满足某些条件的多项式不是置换多项式。类似黎曼假设也可用来证明某些多项式是置换多项式。

1966年[12]，卡里兹和韦尔斯用类似黎曼假设证明

定理3·29 设$e>1$，$e|(q-1)$，当q充分大时，存在$a\in F_q$使得$f=x^c(x^{\frac{q-1}{e}}+a)^k$是$F_q$的置换多项式对所有$(c,q-1)=1,k\geqslant 1$均成立。

用他们的方法，还可证更一般的

定理3·30 设$e>1$，$e|(q-1)$，$g(x)$是F_q上次数大于零的多项式。当q充分大时，存在$a\in F_q$使得$f=x^c(g(x^{\frac{q-1}{e}})+a)^k$是$F_q$的置换多项式对所有满足$k\geqslant 1$，$(c,q-1)=1$均成立。

5. 完备映射

设$f\in F_q[x]$。如果$f(x)$，$f(x)+x$均为F_q的置换多项式，则称f是F_q的完备映射多项式，简称完备映射。这个概念是由曼在1942年研究正交拉丁方的构造时引入的。到目前为止，关于完备映射的结果尚不很多，本节介绍一些主要的结果。

因为置换多项式已有一些判别的方法，从理论上讲，完备映射已有了判别的方法。但从这个角度去判别完备映射，常常是很复杂的。下面的

定理给出了完备映射的一个简洁而有趣的性质。

定理3·31 设$q>3$，则F_q的任何完备映射多项式的简化次数不超过$(q-3)$。

证 先证q为奇数的情形，此时比较容易。设f是F_q的一个完备映射，则f，$f+x$都是F_q的置换多项式。由厄米特准则知，$f(x)$，$f(x)^2$，$(f(x)+x)^2$模(x^q-x)的简化次数都不超过$q-2$。再利用等式

$$(f(x)+x)^2=f(x)^2+2xf(x)+x^2 \tag{3.14}$$

得$f(x)$的简化次数不超过$(q-3)$。

下面证明q为偶数的情形，此时有$q=2^k$。熟知，有限域F_q同构于某一代数整数环E的剩余类环$E/2E$。设η是E到$F_q=E/2E$的标准环同态。令$\eta(x)=x$，则η可扩充为$E[x]$到$F_q[x]$的一个环同态，该环同态仍记为η。取g是F_q的一个生成元，g_1是g在η下的一个逆象，则有

$$g_1^{q-1}\equiv 1 \pmod 2,\quad g_1^{i}\not\equiv \pmod 2 \qquad (0<i<q-1) \tag{3.15}$$

如果$g_1^{q-1}\not\equiv 1 \pmod 4$，则因为有如下的等式

$$\left(g_1\left(1+2\left(\frac{g_1^{q-1}-1}{2}\right)\right)\right)^{q-1}$$

$$\equiv g_1^{q-1}+2g_1^{q-1}(q-1)\,\frac{g_1^{q-1}-1}{2}$$

$$\equiv 1+2\left(\frac{g_1^{q-1}-1}{2}\right)-2g_1^{q-1}\left(\frac{g_1^{q-1}-1}{2}\right)$$

$$\equiv 1 \pmod{4} \tag{3.16}$$

和

$$\eta\left(g_1\left(1+2\left(\frac{g_1^{q-1}-1}{2}\right)\right)\right)=\eta(g_1)=g \tag{3.17}$$

不失一般，我们可设

$$g_1^{q-1}\equiv 1 \pmod{4} \tag{3.18}$$

令$S=\{g_1^i \mid 0\leqslant i\leqslant q-2\}\cup\{0\}$。如果$f=a_{q-2}x^{q-2}+a_{q-3}x^{q-3}+\cdots+a_0(a_i\in F_q)$是$F_q$的完备映射（据厄米特准则，可设$f$具有这种形状），设$F(x)=b_{q-2}x^{q-2}+b_{q-3}x^{q-3}+\cdots+b_0(b_i\in E)$是$f(x)$的一个逆象，则易见

$$\{\eta(F(x)\mid x\in S\}=\{\eta(F(x)+x)\mid x\in S\}$$
$$=F_q$$

因此有

$$\sum_{x\in S}F^2(x)=\sum_{x\in S}(x+2\cdot G(x))^2 \tag{3.19}$$

其中当$x\in S$时，$G(x)\in E$。（3.19）可进一步简化得

$$\sum_{x\in S}F^2(x)\equiv\sum_{x\in S}x^2 \pmod{4}$$
$$=\frac{g_1^{2(q-1)}-1}{g_1^2-1}$$

$$\equiv 0 \pmod{4} \qquad (3.20)$$

同样有（因$F(x)+x$也是置换多项式）

$$\sum_{x\in S}(F(x)+x)^2 \equiv 0 \pmod{4} \qquad (3.21)$$

从

$$0\equiv \sum_{x\in S}(F(x)+x)^2 = \sum_{x\in S}F(x)^2$$

$$+\sum_{x\in S}x^2+2\sum_{x\in S}xF(x)$$

$$\equiv 0+0+2\sum_{x\in S}b_{q-2}x^{q-1}$$

$$\equiv -2b_{q-2} \pmod{4}$$

得出$b_{q-2}\equiv 0 \pmod{2}$。因此$a_{q-2}=\eta(b_{q-2})=0$，即 f 的简化次数不超过$(q-3)$。□

1982年[35]，利德奈特和鲁宾逊提出了定理3·31，并证明了 q 为奇数的情形。他们把 q 为偶数的情形作为一个遗留问题提了出来，这个问题最近被作者之一解决，见〔5〕。

定理3·31在某种意义下是最佳的。例如，x^4+3x是F_7的完备映射，其简化次数为$4=7-3$。又如，$f=ax(a\neq 0,1)$是F_4的完备映射，其简化次数为$1=4-3$。

定理3·32 如果 f 是F_q的完备映射，则

（i）对$a,b\in F_q$，$f(x+a)+b$均是 F_q 的完备映射。

(ii) 对$a\in F_q^*$，$af(a^{-1}x)$是F_q的完备映射。

(iii)若$h(x)\in F_q[x]$是$f(x)$的逆映射，则$h(x)$也是F_q的完备映射。

证 (i) $f(x+a)+b$显然是置换多项式。因$f(x)+x$也是置换多项式，故$f(x+a)+b+x=(f(x+a)+x+a)+b-a$也是置换多项式。(i)成立。

(ii) 记$f^{(a)}(x)=af(a^{-1}x),g(x)=f(x)+x$。则$f^{(a)}(x)+x=af(a^{-1}x)+aa^{-1}x=ag(a^{-1}x)$。因此，$f^{(a)}(x)$，$f^{(a)}(x)+x$均为$F_q$的置换多项式。(ii)成立。

(iii) h显然是F_q的置换多项式。又因$h(c)+c=h(c)+f(h(c))=g(h(c))$对所有$c\in F_q$均成立，故$h(x)+x$也是$F_q$的置换多项式。(iii)成立。□

利用迪克逊的置换多项式表，利德奈特和鲁宾逊也给出了次数不超过5的“标准形”完备映射多项式表。

在本章第二节中，给出了置换多项式的各种构造，这些结果可用来构造完备映射的例子。下面介绍由二项式和迪克逊多项式组成的完备映射。

定理 3·33 设q为奇数，$M(q)$是F_q中形

如$ax^{\frac{q+1}{2}}+bx(a\neq 0)$的完备映射的个数，则有

$$M(q)=\left(\frac{q-1}{2}-\frac{1}{2}\left(1+\left(\frac{-1}{q}\right)\right)\right)\left(\frac{q-3}{2}-\frac{1}{2}\left(1+\left(\frac{-1}{q}\right)\right)\right),$$

其中

$$\left(\frac{-1}{q}\right)=\begin{cases}1, & \text{当} q\equiv 1 \pmod 4 \text{时},\\ -1, & \text{当} q\equiv -1 \pmod 4 \text{时}.\end{cases}$$

证 设$b=at$。由定理3·10知$f(x)=ax^{\frac{q+1}{2}}+bx=ax^{\frac{q+1}{2}}+atx$是$F_q$的完备映射当且仅当下面两个式子同时成立。

$$t=\frac{1+c^2}{1-c^2},\quad c^2\neq 1,\ 0 \tag{3.22}$$

$$\frac{at+1}{a}=t+\frac{1}{a}=\frac{1+d^2}{1-d^2},\quad d^2\neq 1,0 \tag{3.23}$$

上述两个式子又等价于

$$\frac{1}{a}=\frac{1+d^2}{1-d^2}-\frac{1+c^2}{1-c^2},\quad c^2\neq 1,0,\ d^2\neq 1,0,c^2\neq d^2$$

因此

$$M(q)=|\{\{c^2,d^2\}\,|\,c^2\neq 1,0,d^2\neq 1,0,c^2\neq d^2\}|$$

c^2共有$\left(\frac{q-1}{2}-\frac{1}{2}\left(1+\left(\frac{-1}{q}\right)\right)\right)$种取法，在$c^2$

取定后，d^2共有$\left(\frac{q-1}{2}-1-\frac{1}{2}\left(1+\left(\frac{-1}{q}\right)\right)\right)$种取法。于是

$$M(q)=\left(\frac{q-1}{2}-\frac{1}{2}\left(1+\left(\frac{-1}{q}\right)\right)\right)\left(\frac{q-3}{2}-\frac{1}{2}\left(1+\left(\frac{-1}{q}\right)\right)\right)\square$$

设$a\in F_q^*$，$S_a=\{ax^{\frac{q+2}{2}}+bx|b\in F_q\}$，则诸$S_a$把形如$ax^{\frac{q+1}{2}}+bx(a\neq 0)$的二项式化分成$(q-1)$个多项式类。定理3·33表明大约有$\frac{q^2}{4}$个完备映射分布在这$(q-1)$个多项式类中，那么这种分布是否是均匀？用类似黎曼假设可以证明这种分布确是均匀的，即有

定理3·34 设$a\in F_q^*$，$M_a(q)$表示多项式类S_a中完备映射的个数。则有

$$M_a(q)=\frac{q}{4}=O(\sqrt{q})\qquad(3.24)$$

特别，形如$x^{\frac{q+1}{2}}+bx$的完备映射的个数是$\frac{q}{4}+O(\sqrt{q})$个。

定理3·35 设F_q是满足$q>5$的有限域，则F_q有简化次数大于1的完备映射。

证 当q为奇数时，由定理3·33立得。下面

证明当 q 为偶且$q>5$时，F_q 有4次完备映射。因为F_q上 3 次的首1不可约多项式的个数是$N=\frac{1}{3}(q^3-q)>q^2(q^2>5)$，故存在$F_q$中的一双元素 $\{a_1, a_2\}$以及不同的元素d_1，d_2使 $x^3+a_1x^2+a_2x+d_i(i=1,2)$在$F_q$上是不可约的。作变换$x\longrightarrow x-a_1$得到$F_q$上两个不可约多项式$x^3+bx+c_i(i=1, 2)$，$c_1\neq c_2$。再利用第二节的置换多项式表得

$$f(x)=\frac{1}{(c_2-c_1)}(x^4+bx^2+c_1x)$$

是F_q的一个完备映射。□

当$q\leqslant 5$时，定理3·35不成立，即F_q无简化次数大于1的完全映射。从定理3·31知，只需证明当$q=5$时，不存在二次完备映射。因为当 q 为奇时，二次多项式x^2+ax不是F_q的置换多项式（$x^2+ax=x(x+a)$），故F_q 上不存在二次完备映射。

最近[31]，穆伦和利德奈特考虑了与迪克逊多项式有关的完备映射问题。他们证明了

定理3·36 设$k\geqslant 2$ 是整数，$a, b, c\in F_q$，$ab\neq 0$，F_q的特征是p，$g_k(x,a)$是迪克逊多项式。如果$bg_k(x,a)+cx$是F_q的完备映射，则必有下述条件之一成立：

(i) $k\geqslant 3$，$p|k$。

(ii) $k\geqslant 4$，$p\nmid k, q<(9k^2-27k+22)^2$。

定理3·36可从下述定理推得

定理3·37 在定理3·36的条件下，如果$bg_k(x,a)+cx$是F_q的置换多项式，则必有下述条件之一成立。

(i) $k=3$，$c=3ab$；$q\equiv 2(\bmod 3)$。

(ii) $k\geqslant 3$，$p|k$。

(iii) $k\geqslant 4$，$p\nmid k$，$q<(9k^2-27k+22)^2$。

定理3·37基于类似黎曼假设及下述关于多项式绝对不可性的定理。

定理3·38 设$k\geqslant 2$是整数，$a,c\in F_q$，$ac\neq 0$。则多项式

$$f(x,y)=\frac{x^k-a^ky^{2k}}{x-ay^2}\cdot\frac{x^k-1}{x-1}$$

$$+cx^{k-1}y^{k-1} \qquad (3.25)$$

在下列条件之一成立时是F_q上的绝对不可约多项式。

(i) $k=2$。

(ii) $k=3$，$c\neq 3a$，$p\neq 3$。

(iii) $k\geqslant 4$，$p\nmid k$。

定理3·38中条件（iii）是否可以扩广成“$k\geqslant 4$，k不是特征p的方幂”？这是穆伦和利德奈特提出的一个未被解决的问题。

注 本节中介绍的完备映射可以当作是满足附加条件的置换多项式。关于满足附加条件的置换多项式还有一些工作。如

卡里兹在1960年[9]，哥德伯格在1970年[18]，麦肯纳尔在1963年[30]，证明了这方面的一个重要结果。他们的结果可叙述为

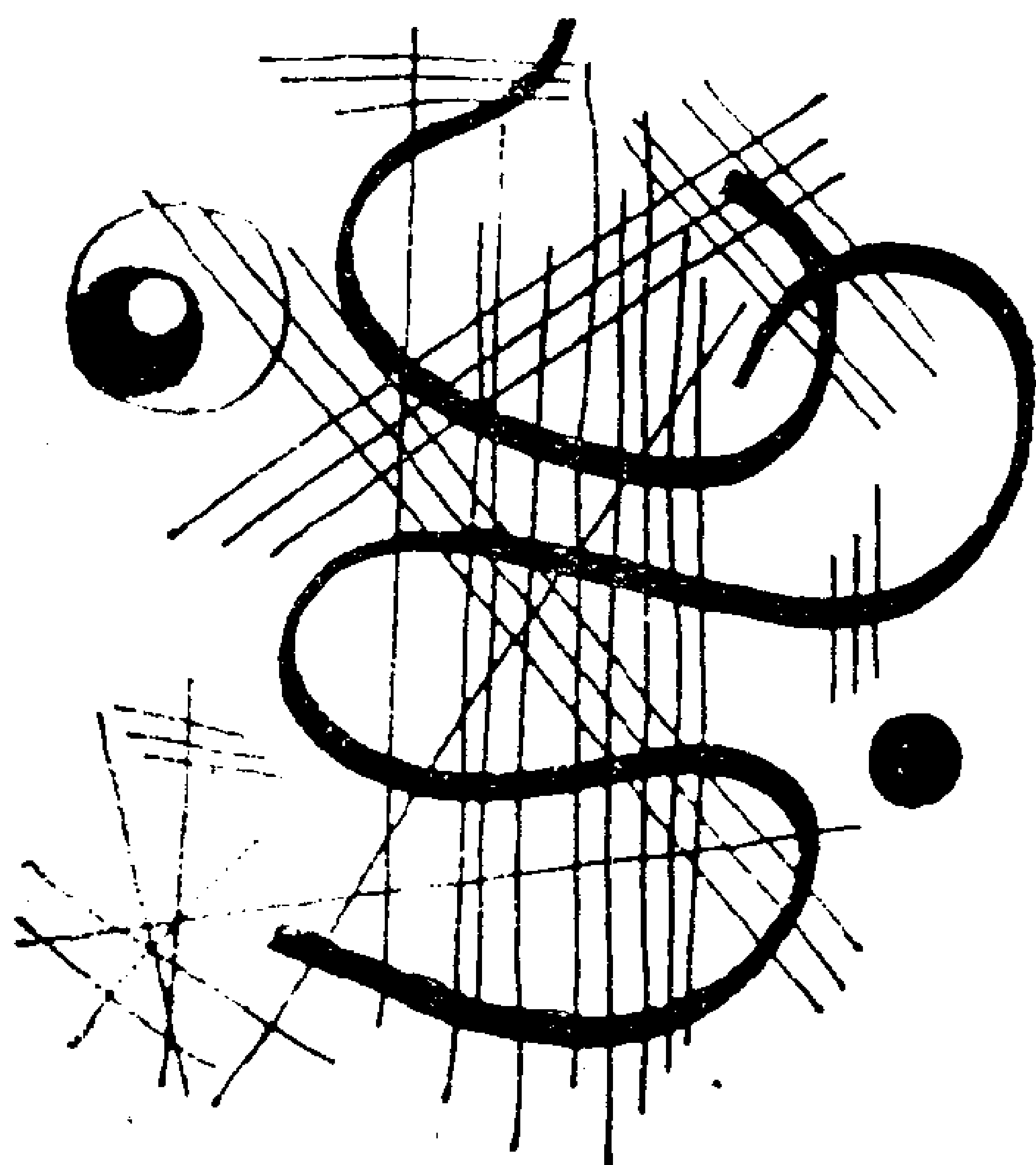
定理3·39　设G是Fq^*的一个真子群，$f \in F_q[x]$，$\deg(f) < q$，则f满足

$$\frac{f(a)-f(b)}{a-b} \in G \tag{3.26}$$

对所有$a, b \in F_q$，$a \neq b$均成立的充要条件是$f(x)=cx^{p^3}+d$，其中$c \in G, d \in F_q, p^j \equiv 1 (\bmod\ m)$，$m$是群$G$在$F_q^*$中的指数。

容易看出，满足（3.26）的多项式是F_q的置换多项式。当$G=F_q$时，（3.26）成立与$f(x)$是F_q的置换多项式等价。

附录　代数基础



1．初等数论

1．任给两个整数a，b，其中$b>0$，如果存在一个整数q使得等式$a=bq$成立，则称b整除a，记作$b|a$，此时a叫做b的倍数，b叫做a的因数。如果b不能整除a，就记作$b\nmid a$。

2．设a，b是两个任给的整数，其中$b>0$，则存在两个唯一的整数q和r，使得

$$a=bq+r,\quad 0\leqslant r<b$$

r称为a模b的最小非负剩余。

3．设$a_1,\cdots,a_n$是n个整数($n\geqslant 2$)，如果整数d是它们之中每一个数的因数，那么d就叫做$a_1,\cdots,a_n$的一个公因数，所有公因数中最大者叫做最大公因数，记作$(a_1,\cdots,a_n)$。如果$(a_1,\cdots,a_n)=1$，就称$a_1,\cdots,a_n$互素。如果m是这n个数的倍数，那么把m叫做这n个数的公倍数，一切公倍数中的最小正数称为最小公倍数，记作$[a_1,\cdots,a_n]$。

4．一个大于1的整数，如果它的因数只有

1 和它本身，这个数就叫做素数，否则就叫做复合数。最小的几个素数是2，3，5，7，11，13，17，19，…。任一个大于1的整数a能够唯一地分解成素数幂之积，即

$$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}, \ \alpha_i>0(i=1,\cdots,k)$$

这里$p_1<p_2<\cdots<p_k$是素数。上式称为a的标准分解式。该结果称为整数的唯一分解定理。

5. 设正整数a，b的标准分解式为

$$a=p_1^{a_1}\cdots p_s^{a_s}, \ a_i\geqslant 0(i=1,\cdots,s)$$

$$b=p_1^{b_1}\cdots p_s^{b_s}, \ b_i\geqslant 0(i=1,\cdots,s)$$

则a和b的最大公因数(a,b)和最小公倍数$[a,b]$可计算如下：

$$(a,b)=p_1^{\min(a_1,b_1)}\cdots p_s^{\min(a_s,b_s)}$$

$$[a,b]=p_1^{\max(a_1,b_1)}\cdots p_s^{\max(a_s,b_s)}$$

其中$\min(a_i,b_i)$，$\max(a_i,b_i)$分别表示a_i,b_i中的最小者和最大者。进一步还有$ab=(a,b)[a,b]$。

6. 给定一个整数$m>0$，如果对两个整数a，b有$m|a-b$，也就是a，b除m后的余数相同，则称a，b模m同余，记作

$$a\equiv b(\mathrm{mod}\ m)$$

以m为模，可以把全体整数按余数来分类，凡用m来除后有相同的余数者都归成同一类。这样，便可把全体整数分成m个类

$$\{0\},\{1\},\cdots,\{m-1\}$$

这些类称为模m的剩余类，它们组成一个有m个元的集合，记为$Z/(m)$。$Z/(m)$作成一个环，称为模m的剩余类环。当$m=p$是素数时，$Z/(p)$还是一个域，也记作F_p。

如果从每一个剩余类中取出一个元$a_i(i=0,1,\cdots,m-1)$，则$\{a_0,a_1,\cdots,a_{m-1}\}$，叫做模$m$的一个完全剩余系。

7．设x是任一实数，用$[x]$表示适合不等式

$$[x]\leqslant x<[x]+1$$

的整数，$[x]$称为x的整数部分，$[x]$实际上就是不超过x的最大整数。在$1,2,\cdots,n$中恰有$\left[\frac{n}{m}\right]$个数是m的倍数。

8．设$\varphi(m)$表示$0,1,\cdots,m-1$，中与m互素的个数，如果$m=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$是$m$的标准分解式，则有

$$\varphi(m)=m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

$\varphi(m)$称为欧拉函数。当$(a,m)=1$时，有

$$a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$$

特别，当$m=p$是素数时，由于$\varphi(p)=p-1$，故

对$(a,p)=1$有

$$a^{p-1}\equiv 1(\mathrm{mod}\ p)$$

此即费马小定理。

9. 设p是素数，a_i是整数，$i=0,1,\cdots,n$，$p\nmid a_n$，则多项式同余式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0(\mathrm{mod}\ p)$$

的解$x(0\leqslant x\leqslant p-1)$的个数不超过$n$，重解按重数计算。

10. 设$m>0$，如果$(n,m)=1$，且同余式

$$x^2\equiv n(\mathrm{mod}\ m)$$

有解，就称n为模m的二次剩余；如果上面的同余式没有解，就称n为模m的二次非剩余。

设$p>2$为素数，共有$\frac{1}{2}(p-1)$个模p的二次剩余，$\frac{1}{2}(p-1)$个模p的二次非剩余，且

$$1^2,2^2,\cdots,(\frac{1}{2}(p-1))^2$$

即为模p的全体二次剩余。

设$p\nmid n$，定义勒让德符号如下：

$$\left(\frac{n}{p}\right)=\begin{cases}1，如果 n 是模 p 的二次剩余，\\-1，如果 n 是模 p 的二次非剩余\end{cases}$$

则有

$$\left(\frac{n}{p}\right)\equiv n^{\frac{p-1}{2}}(\mathrm{mod}\ p)$$

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

$$\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

其中最后一式称为二次互倒律，p，q是不同的奇素数。

11. 设$(a,m)=1$，如果$s>0$，$a^s\equiv1\pmod{m}$，而对于比 s 小的正整数 u，均有$a^u\not\equiv1\pmod{m}$，则称 a 模m的次数是 s。可以证明$s|\varphi(m)$。当$s=\varphi(m)$时，a 叫做模m的原根。m 有原根的充分必要条件是$m=2,4,p^k,2p^k$，其中$k\geqslant1$，p是奇素数。当 p 是素数时，同余式

$$x^s\equiv1\pmod{p}$$

的解数是$(s,p-1)$。

12. 设$m_1,\cdots,m_k$是k 个两两互素的正整数，$M=m_1\cdots m_k$，$M_i=\dfrac{M}{m_i}$，则同余式组

$$\begin{aligned}x&\equiv b_1\pmod{m_1}\\x&\equiv b_2\pmod{m_2}\\&\vdots\\x&\equiv b_k\pmod{m_k}\end{aligned}$$

有唯一解$x=M_1'M_1b_1+\cdots+M_k'M_kb_k\pmod{M}$，其中$M_i'$满足

$$M_i'M_i\equiv1\pmod{m_i}\ (1\leqslant i\leqslant k)$$

上述结果即为著名的孙子定理。

13．阶乘函数定义为$m!=m(m-1)\cdots 2\cdot 1$． $0!=1$．设a，b是非负整数，定义二项系数

$$\binom{b}{a}=\frac{b!}{a!(b-a)!}$$

利用这个符号，二项式的方幂$(x+y)^n$可展开为

$$(x+y)^n=\sum_{i=0}^{n}\binom{n}{i}x^i y^{n-i}$$

14．卢卡斯引理．设m，n是两个正整数，p是一个素数，

$$m=a_0+a_1p+\cdots+a_kp^k\ (0\leqslant a_i\leqslant p-1)$$

$$n=b_0+b_1p+\cdots+b_kp^k\ (0\leqslant b_i\leqslant p-1)$$

是它们的p进位展开式，则有

$$\binom{m}{n}\equiv\binom{a_0}{b_0}\binom{a_1}{b_1}\cdots\binom{a_k}{b_k}\pmod{p}$$

2．群，环，域

1．设G是一个非空集，G上定义了一个二元运算*，满足下列性质：

(i)结合律 对任何a，b，$c\in G$有

$$a*(b*c)=(a*b)*c$$

(ii)存在G中的单位元e满足，对任何$a\in G$，

$$a*e=e*a=a$$

(iii)对任何$a\in G$，存在一个逆元$a^{-1}\in G$使

$$a*a^{-1}=a^{-1}*a=e$$

满足上面三个条件的集合G称为一个群。如果G还满足

(iv)对任何a，$b\in G$有

$$a*b=b*a$$

则称G是阿贝尔群（即交换群）。

如果在群G中存在一个元素g，使得对任何$a\in G$都存在一个整数j，使得$a=g^j$，则称g是G的一个生成元，称G为一个循环群。

如果群G只含有限个元，称G为有限群，G中元素的个数称为G的阶，通常用$|G|$表示。

如果G是一个n阶循环群，g是G的一个生成元，$g_1=g^j$，则g_1也是G的生成元当且仅当$(j,n)=1$。

如果G的一个子集H在G的运算下也作成一个群，就称H为G的子群。定义

$$aH=\{ah|h\in H\}$$

则所有aH把G分成若干个不相交的子集。每一子集aH称为G关于H的一个左陪集。类似地定义

$$Ha=\{ha|h\in H\}$$

Ha称为G关于H的右陪集。如果H是G的一个有限子群，则每一个左陪集和右陪集的元素个数相

同。G关于H的左陪集（或右陪集）的个数称为H在G中的指数，记为$[G:H]$。易见$|G|=|H|\cdot[G:H]$。

设$f: G\longrightarrow H$是群G到群H的一个映射，如果对任何a，$b\in G$均有

$$f(a\times b)=f(a)\cdot f(b)$$

即f保持G的运算，则称f是群G到群H的一个同态。如果f是满射，即H中每一元都是G中某一元的象，则称f是满同态；如果f是单射，即当$a\neq b$时，$f(a)\neq f(b)$，则称f是单同态。即满又单的同态称为同构，此时G和H称为同构的群，当$G=H$时，f称为G的自同态。

如果对所有$a\in G$，$h\in H$（G的子群），都有$aha^{-1}\in H$，则称H为G的正规子群。子群H在G中是正规的当且仅当任一左陪集aH和右陪集Ha相等。这样，对正规子群，陪集之间可以定义运算：

$$(aH)(bH)=(ab)H$$

在这种运算下，所有H的陪集作成一个群，记为G/H，称为G关于H的商群。$|G/H|=[G:H]$。定义同态f：$G\longrightarrow G/H$，$f(a)=aH(a\in G)$，f称为G到商群H的标准同态。

2。置换群。设n是一个正整数，如果a_1，$\cdots,a_n$是$1,2,\cdots,n$的一个排列，则称

$$\sigma=\begin{pmatrix}1 & 2\cdots & n\\ a_1 & a_2\cdots & a_n\end{pmatrix}$$

为一个 n 元置换。置换 σ 可以理解为把 i 变换成 a_i，因此是$\{1,2,\cdots,n\}$到自身的一个一一映射。两个置换的复合也是一个置换。所有 n 元置换在复合运算下作成一个群，称为 n 元置换群，常用 S_n表示。S_n的元素个数是$n!$。

以$(a_1a_2\cdots a_k)$表示一种特殊的置换，它把a_1变到a_2，a_2变到a_3，…，a_{k-1}变到a_k，a_k变到 a_1，保持其余数字不变，这样的置换$(a_1\cdots a_k)$ 称为一个长度为 k 的圈。当$k=2$时，称为一个对换，此时(a_1a_2)表示a_1，a_2互变，其余数字不动。

任何一个置换都可分解成若干个对换的乘积（此处乘积为置换群的复合运算）。若一个置换可以表成偶数个对换的积，则称该置换为偶置换，否则称为奇置换。当 k 为奇数时，长度为 k 的圈是偶置换；当 k 为偶时，长度为 k 的圈是奇置换。

所有 n 阶偶置换作成S_n的一个子群，称为交错群，用A_n表示。$[S_n:A_n]=2$。

3。环。设集 R 上有两种运算，加法“+”和乘法“·”，如果 R 满足

(i) R 关于加法运算“+”作成一阿贝尔群，

(ii) R 关于乘法是结合的，即对 $a,b,c\in R$ 有

$$(a\cdot b)\cdot c=a\cdot(b\cdot c)$$

(iii) R 满足分配律，对任何 $a,b,c\in R$ 有

$$a\cdot(b+c)=a\cdot b+a\cdot c$$

$$(b+c)\cdot a=b\cdot a+c\cdot a$$

则称 R 是一个环。环中运算“+”，“·”不一定是通常的加法和乘法。R 关于“+”有一单位元，通常以 0 表示（即零元）。如果 R 关于乘法“·”有单位元，则称 R 是有单位元的环。如果 R 关于乘法是交换的，就称 R 为交换环。如果 R 是有单位元的交换环，且满足 $a\cdot b=0$ 可推出 $a=0$ 或 $b=0$，就称 R 是一个整环。如果环 R 的全体非零元作成一个群，就称 R 为除环。一个交换的除环称为一个域。

例如，剩余类组成的集 $Z/(m)$ 是一个环。当 p 为素数时，$Z/(p)$ 是一个域。

如果环 R 到环 S 的一个映射 φ 满足，对任何 $a,b\in R$ 均有

$$\varphi(a+b)=\varphi(a)+\varphi(b)$$

$$\varphi(ab)=\varphi(a)\cdot\varphi(b)$$

则称 φ 是 R 到 S 的一个同态。若 φ 是既满又单的同态，就称 φ 为一个同构。类似地有两个域同构的概念。

4．域扩张，设 K 是一个域，F 是 K 的一个

子集，如果在K的运算下，F也作成一个域，则称F是K的子域，K是F的扩域。如果$\theta\in K$，θ满足F上的一个多项式方程：

$$a_n\theta^n+a_{n-1}\theta^{n-1}+\cdots+a_0$$
$$=0(a_i\in F, a_n\neq 0),$$

则称θ是F上的代数元。如果K的每一个元都是F上的代数元，就称K是F的代数扩域。

如果$\theta\in K$，θ是F上的代数元，则存在唯一的一个首1不可约多项式$g(x)\in F[x]$，满足$g(\theta)=0$.$g(x)$称为θ在F上的极小多项式，$\deg(g(x))$称为θ在F上的次数。可以证明，$[F(\theta):F]=\deg(g(x))$，这里$F(\theta)$是含F和θ的最小扩域。

F上所有代数元作成一个域，称为F的代数闭包，或代数闭域，记为$\overline{F}$。显然，$\overline{F}$是F的扩域。

3. 有限域

1. 由有限个元素组成的域叫做有限域。可以证明，任一有限域的元素个数q是一个素数p的方幂p^k，记$q=p^k$。反之，对任给的素数p，和正整数k，存在元素个数为p^k的有限域。任何两个q阶有限域是同构的。在同构意义下唯一的有限域均用F_q表示。在有限域中，特征是指最小的正

整数 r 使得对任何$a\in F_q$均有

$$r\cdot a=a+a+\cdots+a\ (\text{共 } r \text{ 个})\ =0$$

因此，F_q的特征是p，在F_q中有恒等式

$$(x+y)^p=x^p+y^p$$

2. 如果$a\in F_p$，则有$a^q=a$。于是多项式(x^q-x)可以分解成线性因子之积

$$x^q-x=\prod_{a\in F_q}(x-a)$$

3. 对任一有限域F_q，F_q的乘群$F_q{}^*$（由F_q的全体非零元组成）是一个$(q-1)$阶循环群。$F_q{}^*$的一个生成元称为F_q的本原元。

4. 设K是含F_q的一个有限域，则K含有q^m个元素，其中$m=[K:F_q]$。因此，必有$K=F_{q^m}$。

5. 如果$q=p^n$，则F_q的每一个子域的阶为p^m，其中$m|n$；反之，如果m是n的一个正因子，则存在F_q的唯一一个有p^m个元的子域。

6. 对每一有限域F_q，和正整数n，存在一个$F_q[x]$的n次不可约多项式。如果$f\in F_q[x]$是F_p上的一个m次不可约多项式，则$f(x)$整除$x^{q^n}-x$当且仅当$m|n$。$F_q[x]$中的n次首1不可约多项式的个数

$$N_q(n)=\frac{1}{n}\sum_{d|n}\mu\left(\frac{n}{d}\right)q^d$$

$$=\frac{1}{n}\sum_{d\mid n}\mu(d)q^{\frac{n}{d}}$$

这里$\mu(d)$是麦比乌斯函数，定义如下：

$$\mu(d)=\begin{cases}1, & \text{如果}n=1,\\ (-1)^k, & \text{如果}n\text{是}k\text{个不同素数的积},\\ 0, & \text{如果}n\text{被一个素数的平方整除}.\end{cases}$$

如果f是$F_q[x]$的一个m次不可约多项式，则f在F_{q^m}中有一根α，且f的全部根都是单根，由$\alpha,\alpha^q,\alpha^{q^2},\cdots,\alpha^{q^{m-1}}$给出。于是$f$在$F_p$上的分裂域由$F_{q^m}$给出，$F_q$上两个$m$次不可约多项式的分裂域是同构的，此外不可约多项式$f$在$F_q$上的分裂域是指含$F_q$及$f$的所有根的最小扩域。

7．设F_{q^m}是F_q的一个扩域，$\alpha\in F_{q^m}$，则元素$\alpha,\alpha^q,\cdots,\alpha^{q^{m-1}}$，称为$\alpha$关于$F_q$的共轭。所有$\alpha$的共轭在$F_{q^m}$中有相同的阶。如果$\alpha$是$F_{q^m}$的一个本原元，则$\alpha,\alpha^q,\cdots,\alpha^{q^{m-1}}$均是$F_{q^m}$的一个本原元。定义$\sigma_j(\alpha)=\alpha^{q^j}$，则易见$\sigma_j$是$F_{q^m}$关于$F_q$的一个自同构。$F_{q^m}$关于$F_q$的全体自同构由$\sigma_0,\sigma_1,\cdots,\sigma_{m-1}$组成，这些自同构在合成运算下作成一个$m$阶循环群，其中$\sigma=\sigma_1$是一个生成元。因此对$\alpha\in F_{q^m}$有$\alpha\in F_q$当且仅当$\sigma(\alpha)=\alpha$。

8．设$f(x)$是模p的一个n次不可约多项式，则重模剩余类环

$$Z[x]/(f(x))\ (\mathrm{mod}\ p)$$

正好是p^n阶的有限域。

4. 多项式

1. 设F是一域，形如$\sum_{i=0}^{n}a_i x^i\ (a_i\in F)$的表达式称为$F$上的多项式，所有这种多项式作成一个环，记为$F[x]$. 类似于本附录第1部分中整数的情形，可定义多项式的整除性，素多项式(即不可约多项式)，最大公因子，最小公倍式等概念。

2. 设$g\neq 0$是$F[x]$中的一多项式，则对任何$f\in F[x]$，存在$F[x]$中的多项式q_1和r_1使得

$$f=q_1g+r_1,\quad \deg(r_1)<\deg(g_1)$$

同样有

$$g=q_2r_1+r_2,\quad \deg(r_2)<\deg(r_1)$$

$$r_1=q_3r_2+r_3,\quad \deg(r_3)<\deg(r_2)$$

$$\vdots$$

$$r_{s-2}=q_sr_{s-1}+r_s,\quad \deg(r_s)<\deg(r_{s-1})$$

$$r_{s-1}=q_{s+1}r_s$$

其中$q_1,\cdots,q_{s+1},r_1,\cdots,r_s$都是$F[x]$中的多项式。$r_s$就是$f$和$g$的最大公因式。

上述算法称为欧几里得算法。

3. $F[x]$中次数大于零的任何多项式可以唯

一（除次序外）地写成下述形式

$$f = ap_1^{e_1} \cdots p_k^{e_k}$$

其中$a \in F$，$p_1, \cdots, p_k$是$F[x]$中的首1不可约多项式，$e_1, \cdots, e_k$是正整数。

4．设$f \in F[x]$，则剩余类环$F[x]/(f)$是一个域当且仅当f在F上是不可约的。

5．如果$f(x) = a_0 + a_1 x + \cdots + a_n x^n$，定义导数$f'(x) = a_1 + 2a_2 x + \cdots + na_n x^{n-1} \in F[x]$．则$b \in F$是$f \in F[x]$的一个重根当且仅当$b$是$f$和$f'$的根．如果$(x-b)^k | f(x)$，$(x-b)^{k+1} \nmid f(x)$，则称$b$是$f$的$k$重根。任何一个$n(n>0)$次多项式在$F$中至多有$n$个根（重根按重数计算）．

6．对$n \geqslant 0$，设$a_0, a_1 \cdots, a_n$是$(n+1)$个不同的元素（均在F中），$b_0, b_1, \cdots, b_n$也是F的$(n+1)$个元素(可以相同)，则在$F[x]$中恰有一个n次多项式f满足$f(a_i) = b_i (i = 0, 1, \cdots, n)$，这个多项式为

$$f(x) = \sum_{i=0}^{n} b_i \prod_{\substack{k=0 \\ k \neq i}}^{n} (a_i - a_k)^{-1} (x - a_k)$$

$f(x)$称为拉格朗日插值公式。

7．设$x_1, \cdots, x_n$是n个变元，记

$$\sigma_1 = x_1 + x_2 + \cdots + x_n$$

$$\sigma_2 = x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n + x_2 x_3 + \cdots + x_{n-1} x_n$$

$$\vdots$$

$$\sigma_n = x_1x_2\cdots x_n$$

一般地有

$$\sigma_k = \sigma_k(x_1,\cdots,x_n) = \sum_{1\leqslant i_1<\cdots<i_k\leqslant n} x_{i_1}\cdots x_{i_k} \quad (k=1,\cdots,n)$$

σ 称为变元$x_1,\cdots,x_n$的第 i 个初等对称多项式。

又记

$$s_k = s_k(x_1,\cdots,x_n) = x_1^k + \cdots + x_n^k \quad (k\geqslant 1)$$

则有华林公式

$$s_k = \sum (-1)^{i_2+i_4+i_6+\cdots} \frac{(i_1+i_2+\cdots+i_n-1)!k}{i_1!i_2!\cdots i_n!} \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_n^{i_n}$$

其中$k\geqslant 1$，和式是对所有满足$i_1+2i_2+\cdots+ni_n=k$的 n 元非负整数组$(i_1,\cdots,i_n)$进行的。

s_k和σ_i之间的另一个关系是牛顿公式：

$$s_k - s_{k-1}\sigma_1 + s_{k-2}\sigma_2 + \cdots + (-1)^{m-1}s_{k-m+1}\sigma_{m-1} + (-1)^m \frac{m}{n} s_{k-m}\sigma_m = 0$$

其中$k\geqslant 1$，$m=\min(k,n)$。

8．设ξ是域F的某个扩域中的一个 n 次本

原单位根，则所有 n 次本原根为 $\xi^s(1\leqslant s\leqslant n,(s,n)=1)$，定义 n 次分圆多项式为

$$\Omega_n(x)=\prod_{\substack{(s,n)=1\\1\leqslant s\leqslant n}}(x-\xi^s)$$

则有

$$x^n-1=\prod_{d\mid n}\Omega_d(x)$$

当 F 是有理数域 Q 时，$\Omega_n(x)$ 是 Q 上的 $\varphi(n)$ 次整系数不可约多项式，此处 $\varphi(n)$ 是欧拉函数。

9．设 $f\in F_q[x,y]$，如果 f 在 $\overline{F_q}[x,y]$ 中也是不可约的，就称 f 是 F_q 上的绝对不可约多项式，此处 $\overline{F_q}$ 为 F_q 的代数闭包。

设 $f(x,y)=g_0y^d+g_1(x)y^{d-1}+\cdots+g_d(x)\in F_q[x,y]$，其中 g_0 是非零常数。令

$$\psi(f)=\max_{1\leqslant i\leqslant d}\frac{1}{i}\deg(g_i)$$

如果 $\psi(f)=\dfrac{m}{d}$，且 $(d,m)=1$，则可以证明 $f(x,y)$ 是 F_q 上的绝对不可约多项式。

10．应用有限域上的类似黎曼假设，可以证明下述的兰——魏依定理：

假设 $f(x,y)\in F_q[x,y]$ 是次数大于 d 的绝对不可约多项式，则存在一个常数 $c(d)$，使得

$$|N(f)-q|\leqslant(d-1)(d-2)\sqrt{q}+c(d)$$

其中$N(f)$表示方程

$$f(x,y)=0$$

在F_q中的解数。

参 考 文 献

〔1〕华罗庚，《数论导引》，科学出版社，1957。

〔2〕柯召，孙琦，《初等数论一百例》，上海教育出版社，1980。

〔3〕柯召，孙琦，《数论讲义》，上册，高等教育出版社，1986。

〔4〕丘维声，n元全差置换的数目，科学通报，22（1985），1756—1757。

〔5〕万大庆，On a problem of Niederreiter and Robinson about finitefields, J. Austral. Math.Soc.serA,14(1986)；（摘要），科学通报，8（1985），636。

〔6〕万大庆，On a conjectur of Carlitz, J.Austral.Math.Soc.SerA(to appear);科学通报，1（1986），79—80。

〔7〕万大庆，Permutation binomials of finite fields;

〔8〕Bombierie. E and Davenport, H, On two problems of Mordell, Amer.J.Math.88(1966), 61—70.

〔9〕Carlitz, L, A theorem on permutations in a finite field, Proc. Amer. Math. Soc.

11(1960),456-459.

〔10〕 Carlitz, L, Some theorems on permutation polynomials, Bull. Amer. Math. Soc.68 (1962), 120-122.

〔11〕 Carlitz. L and Lutz. J. A, A characterization of permutation polynomials over finite fields, Amer. Math. Monthly. 85 (1978), 746-748.

〔12〕 Carlitz, L and Wells, c, The number of solutions of a special system of equations in a finite field, Acta Arith, 12(1966), 77-84.

〔13〕 Chowla, S, and Zassenhaus, Some conjectures concerning finite fields,Norske Vid. Selsk. Forh (Trondheim), 41(1968), 34-35.

〔14〕 Cohen, S. D, The distribution of polynomials over finite, Acta Arith, 17 (1970), 255-271.

〔15〕 Davenport, H and Lewis, D. J, Notes on congruences(I),Quart. J,Math.(2)14(1963),51-60.

〔16〕 Dickson, L. E, Linear Groups with an Exposition of the Galois Field Theory, Teuber, Leipzig, 1901; Dover, New York,1958.

〔17〕 Fried, M, On a conjecture of schur, Michigan Math. J., 17(1970),41-55.

〔18〕 Goldberg, M, The group of the quardratic

residue tourement, Canad. Math. Bull., 13 (1970),51-54.

[19] Hayes, D.R, A geometric approach to permutation polynomials over a finite field, Duke Math. J. 34 (1967),293-305.

[20] Kurbatov,V. A, On polynomials which prcduce substitutions for infinitely many primes (Russian), Sverdlovsk, Gos. Ped. Inst. Včen. Zap. 4(1947),79-121.

[21] Kurbatov, V. A, On the monodromy group of an algebraic function (Russian). Mat. sb 25(1949),51-94; Amer. Math. Soc.Transl (2)36 (1964),17-62.

[22] Lang, S and Weil, A, Number of points of varieties in finite fields, Amer. J. Math., 76 (1954), 819-827.

[23] Lausch, H, Müller, W and Nöbauer, W., über die struktur einer durch Dicksonpolynome dargestellten permutations gruppe des Restklassenringos modulo n, J. Reine Angew. Math., 261(1973),88-99.

[24] Lausch, H and Nöbauer, W ., Algebra of Polynomials, North-Holland, Amsterdam , 1973.

[25] Lidl, R and Müller, W., Permutation polynomials in RSA-cryptosystems, Advancps

in Cryptology, Edited by D. Chaum, 1984.

〔26〕 Lidl, R and Niederreiter,H.,On orthogonal systems and permutation polynomials in several variables, Acta Arith., 22 (1973), 257-265.

〔27〕 Lidl, R and Niederreiter, H.,Finite Fields, Encyclopedia. of Math. and Its Appl. vol. 20, Addison-Wesley, Reading Mass. 1983.

〔28〕 Lidl, R and Wells,C., Chebyshev polynomials in several variables,J. Reine Angew. Math. 255(1972),104-111.

〔29〕 Mac Cluer, C. R., On a conjecture of Davenport and Lewis concerning exceptional polynomials, Acta Arith, 12ö(1967),289-299.

〔30〕 Mcconnel, R., Pseudo-ordered polynomials over a finite field, Acta Arith., 8 (1963), 127-151.

〔31〕 Mullen, G. L and Niederreiter, H., Dickson polynomials over finite fields and complete mappings,Canad Math. Bull (to appear).

〔32〕 Müller,W and Nöbauer, W., Some remarks on publickey cryptosystems, Studia Sci. Math. Hungary,16(1981).

〔33〕 Narkiewicz, W., Uniform Distribution of Sequences of Integers in Residue Classes,

Lecture Notes in Math. Springer-Verlag, vol.1087, 1984.

[34] Niederreiter, H and Lo. S. K., Permutation polynomials over rings of algebraic integers. Abh.Math. Sem. Hamburg, 49 (1979), 126-139.

[35] Niederreiter, H and Robinson, K. H., Complete mappings of finite fields, J.Austral. Math. Soc. SerA. 33 (1982), 197-212.

[36] Nöbauer, W, über permutations polynome und permutation functionen für primzahl potenzen, Monatsh.Math. 69 (1965), 230-238.

[37] Nöbauer, W, Polynome, Welche für gegebene Zahler permutations polynome Sind, Acta Arith, 11(1966), 437-442.

[38] Redei, L., über eindeutig umkehrbare polynome in endlichen körpern, Acta Sci. Math (Szeged), 11(1946), 85-92.

[39] Rivest, R., Shamir. A and Adleman, L., A method of obtaining digital signatures and public-key cryptosystem, CACM 21 (1978), 120-126.

[40] Schur, I, über den zusammenhang zwischen einem problem der zahlen theorie und einem Satz über algebrais che Funktionen Sitzungsber, Preuß Acad. Wiss. Berlin Math-Natur-

wiss, KL (1923), 123-134.

〔41〕 Tietäväinen, A, On non-residues of polynomial, Ann. Univ. Turku. Ser AI, 94 (1966), 6 pp.

〔42〕 Wegner, U., über die ganzzahligen polynome, die für unendlich viele primzahl moduln permutationen liefern, Dissertation, Berlin, 1928.

〔43〕 Williams, K.S., On exceptional polynomials, Canad Math. Bull. 11 (1968), 279-282.

〔44〕 孙琦、旷京华，关于代数数域上的完全剩余系，数学学报，2(1987), 226—228.

外国人名索引

Abel	阿贝尔
Adleman	阿德利曼
Betti	伯蒂
Bombieri	朋比利
Carlitz	卡里兹
Chebyshev	切比雪夫
Chowla	乔拉
Cohen	科恩
Davenport	达文波特
Dickson	迪克逊
Dirichlet	狄里克雷
Euclid	欧几里得
Euler	欧拉
Fermat	费马
Fried	弗雷德
Gauss	高斯
Goldberg	哥德伯格
Gwehenberger	格温伯格
Hayes	海斯
Hermite	厄米特
James	詹姆斯

Kurbatov	库尔巴托夫
Lagrange	拉格朗日
Lang	兰
Lausch	劳斯基
Legendre	勒让德
Lewis	刘易斯
Lidl	利德尔
Lo	罗
Lucas	卢卡斯
Lutz	路兹
MacCluer	麦克卢尔
MacConnel	麦肯纳尔
Mann	曼
Mathiew	马修
Möbius	麦比乌斯
Mullen	穆伦
Müller	米勒
Narkiewicz	纳克维兹
Newton	牛顿
Niederreiter	利德奈特
Nöbauer	诺鲍尔
Rédei	里德
Rieamann	黎曼
Rivest	里维斯特
Robinson	鲁宾逊
Roger	罗格尔

Rosochowicz	罗索丘维兹
Schur	舒尔
Shamir	夏米尔
Tietäväinen	蒂特凡林
Wegner	威格纳
Weil	魏依
Wells	韦尔斯
Williams	威廉斯
Zame	泽门
Zassenhaus	查森豪斯